Column2	Column3	Column4	Column5	Column6	Column7
	0				
	Background: Applied Policing and Crime Resolution				
	•□**Purpose**:				
		○ To develop investigative, analytical, and legal skills for resolving crimes.			
		○ To prepare students for roles in law enforcement, forensic analysis, and private investigation.			
	•□**Applications**:				
		○ Crime scene management.			
		○ Evidence collection and analysis.			
		○ Interviewing witnesses and suspects.			
	Key Topics in Applied Policing and Crime Resolution				
	1. Crime Scene Management				
	•□**Principles**:				
		○ Securing the crime scene to prevent contamination.			
		○ Documenting the scene through photographs, sketches, and notes.			
	•□**Experimental Applications**:				
		○ Simulate a crime scene and practice securing and documenting evidence.			
		○ Analyze mock evidence for fingerprints, DNA, or ballistic data.			
	2. Investigative Techniques				
	•□**Key Concepts**:				
		○ Conducting preliminary investigations.			
		○ Using surveillance and undercover operations.			
	•□**Experimental Applications**:				
		○ Role-play scenarios for interviewing witnesses and suspects.			
		○ Practice using surveillance equipment like cameras and GPS trackers.			
	3. Evidence Handling and Analysis				
	•□**Principles**:				
		○ Proper collection, labeling, and storage of evidence.			

- Chain of custody to ensure evidence integrity.

•□**Experimental Applications**:

- Perform forensic analysis on mock evidence (e.g., blood samples, fibers).
- Use tools like microscopes and chromatography for detailed examinations.

4. Legal Framework

•□**Key Topics**:

- Understanding the Criminal Procedure Act and Evidence Act.
- Applying constitutional rights during investigations.

•□**Experimental Applications**:

- Mock trials to practice presenting evidence in court.
- Analyze case studies to identify legal and procedural errors.

5. Crime Prevention Strategies

•□**Principles**:

- Community policing to build trust and gather intelligence.
- Using data analytics to predict and prevent crimes.

•□**Experimental Applications**:

- Develop crime prevention plans for specific scenarios.
- Use software tools to analyze crime patterns and hotspots.

Applications in Law Enforcement

1. Forensic Investigation:

- Analyze evidence to reconstruct crime scenes.

2. Criminal Profiling:

- Use psychological and behavioral analysis to identify suspects.

3. Community Engagement:

- Build partnerships with local communities to prevent and solve crimes.

Would you like to explore specific experimental setups, tools, or advanced techniques in these areas? Let's dive deeper into

The **Applied Policing and Crime Resolution** fields outlined within **NATED and NCV programs** are rich in analytical tech

Advanced Calculations in Applied Policing and Crime Resolution

1. Evidence Decay Over Time Using Exponential Models

Physical evidence, such as DNA or chemical residues, decays over time, which can be modeled using exponential decay:

$$C(t)=C0e−λt,C(t) = C_0 e^{-\lambda t},$$

where:

- C(t)C(t): Concentration of evidence at time tt,
- C0C_0: Initial concentration,
- λ\lambda: Decay constant.

1. Concentration after 10 days:

$$C(10)=100e−0.02·10=100e−0.2≈81.87 ng.C(10) = 100 e^{-0.02 \cdot 10} = 100 e^{-0.2} \approx 81.87 \, \text{ng}.$$

2. Projectile Motion in Ballistic Analysis

When investigating a shooting, the path of a projectile can be modeled by:

$$y=xtanθ−gx22v2cos2θ,y = x \tan \theta - \frac{g x^2}{2 v^2 \cos^2 \theta},$$

where:

- yy: Vertical displacement,
- xx: Horizontal displacement,
- θ\theta: Firing angle,
- vv: Initial velocity,
- gg: Acceleration due to gravity (9.8 m/s29.8 \, \text{m/s}^2).

Example: Given v=500 m/sv = 500 \, \text{m/s}, θ=30∘\theta = 30^\circ, and x=100 mx = 100 \, \text{m}:

1. Height (yy):

y=100tan30∘−9.8·10022·5002·cos230∘.y = 100 \tan 30^\circ - \frac{9.8 \cdot 100^2}{2 \cdot 500^2 \cdot \cos^2 30^\circ}.

2. Compute:

y≈57.7−0.27=57.43 m.y \approx 57.7 - 0.27 = 57.43 \, \text{m}.

3. Area Estimation for Crime Scene Management

Using calculus, calculate the area of irregular crime scene perimeters. Divide the boundary into segments described by functi

A=∫x1x2y(x) dx.A = \int_{x_1}^{x_2} y(x) \, dx.

Example: For a boundary described by y(x)=x2+2y(x) = x^2 + 2 between x=0x = 0 and x=3x = 3:

1. Compute area:

A=∫03(x2+2) dx=[x33+2x]03.A = \int_0^3 (x^2 + 2) \, dx = \left[\frac{x^3}{3} + 2x\right]_0^3.

2. Result:

A=(273+6)−0=15 m2.A = \left(\frac{27}{3} + 6\right) - 0 = 15 \, \text{m}^2.

4. Surveillance Analysis Using Camera Rotation

The angular velocity of a surveillance camera can be modeled as:

θ(t)=ωt+12αt2,\theta(t) = \omega t + \frac{1}{2} \alpha t^2,

where:

- θ(t)\theta(t): Angle rotated,
- ω\omega: Initial angular velocity,
- α\alpha: Angular acceleration.

Example: If ω=0.5 rad/s\omega = 0.5 \, \text{rad/s}, α=0.1 rad/s2\alpha = 0.1 \, \text{rad/s}^2, find the angle after t=10 st =

$$\theta(10) = 0.5 \cdot 10 + \frac{1}{2} \cdot 0.1 \cdot 10^2 = 5 + 5 = 10 \, \text{rad}.$$

5. Predictive Analytics for Crime Prevention

Using linear regression to predict crime patterns:

$$y = mx + b,$$

where:

- yy: Predicted crime rate,
- xx: Variable (e.g., population density),
- mm: Slope of the trendline,
- bb: Intercept.

Example: If m=0.02 crimes/personm = 0.02 \, \text{crimes/person}, b=10b = 10:

1. For x=1000x = 1000:

$$y = 0.02 \cdot 1000 + 10 = 30 \, \text{crimes}.$$

Applications in Crime Resolution and Prevention

1. Forensic Investigations:

- Use ballistic and decay models to reconstruct crime scenes.

2. Crime Scene Management:

- Employ area estimation to secure and document crime perimeters.

3. Predictive Policing:

- Apply regression models and data analytics to forecast and prevent crimes.

Would you like further details on any mathematical model, or should we dive into experimental tools used in these areas? Le

The **NATED and SAQA NQF programs** provide structured learning pathways for various fields, including **police manage**

1. Management Information Systems in Policing

Background:

- Management Information Systems (MIS) in policing are designed to collect, analyze, and disseminate crime data f
- Applications include crime mapping, resource tracking, and performance monitoring.

Experimental Applications:

- Simulate crime data entry and analysis using MIS tools.
- Develop crime heatmaps to identify hotspots and allocate patrols effectively.

2. Incident Collision Scenarios

Background:

- Focuses on investigating road traffic collisions to determine causes and prevent future incidents.
- Includes analyzing human, vehicle, and environmental factors.

Experimental Applications:

- Recreate collision scenarios to study impact dynamics.
- Use simulation software to analyze vehicle trajectories and collision points.

3. Research Methods for Conducting Patrols

Background:

- Patrol methods aim to prevent crime and enhance public safety through visible police presence.
- Research involves optimizing patrol routes and schedules.

Experimental Applications:

- Design patrol routes using Geographic Information Systems (GIS).
- Conduct randomized patrol experiments to measure crime reduction.

4. Community Policing and Communication Skills

Background:

- Community policing emphasizes collaboration between police and communities to solve problems and build trust.
- Effective communication skills are essential for engaging with diverse populations.

Experimental Applications:

- Role-play scenarios to practice conflict resolution and active listening.
- Develop community engagement plans to address specific safety concerns.

5. Operational Performance in Traffic Management

Background:

- Traffic management involves optimizing road safety and flow through enforcement and education.
- Operational performance measures include response times and accident reduction rates.

Experimental Applications:

- Analyze traffic flow data to identify bottlenecks.
- Implement traffic enforcement strategies and measure their effectiveness.

6. Principles of Police Investigation

Background:

- Investigative principles include evidence preservation, chain of custody, and impartiality.
- Focuses on systematic approaches to solving crimes.

Experimental Applications:

- Conduct mock crime scene investigations to practice evidence collection.
- Use forensic tools to analyze fingerprints, DNA, and ballistic evidence.

7. Study Material for Police Firearms

Background:

- Covers firearm handling, safety, and competency testing.
- Includes theoretical knowledge and practical training.

Experimental Applications:

- Practice firearm handling and target shooting in controlled environments.
- Study ballistic properties and their application in investigations.

Applications Across Fields

1. **Crime Prevention**:
    - Use MIS tools to predict and prevent crimes.
2. **Traffic Safety**:
    - Develop strategies to reduce road accidents and improve enforcement.
3. **Community Engagement**:
    - Build partnerships with local organizations to enhance public safety.

Would you like to explore specific experimental setups, advanced calculations, or study materials for any of these topics? Le

Delving into **calculus** applications, especially integrals and derivatives, within the fields of **policing and related scenarios**,

1. Management Information Systems (MIS): Optimizing Police Patrol

- **Crime Hotspot Modeling Using Integrals**: Crime density in a region can be modeled as a density function f(x,y)f
  - Total crime density in a region RR:

D=∫∫Rf(x,y) dx dy.D = \int\int_R f(x, y) \, dx \, dy.

Example: If f(x,y)=x2+y2f(x, y) = x^2 + y^2 and RR is a circular region with radius 2 centered at the origin:

1. Use polar coordinates (x=rcosθ,y=rsinθx = r \cos \theta, y = r \sin \theta):

D=∫02π∫02(r2) r dr dθ.D = \int_0^{2\pi} \int_0^2 (r^2) \, r \, dr \, d\theta.

2. Compute:

\[D = \int_0^{2\pi} \int_0^2 r^3 \, dr \, d\theta = \int_0^{2\pi} \left[\frac{r^{4}{4}\right]_0^2 d\theta = \int_0^{2\pi} 4 d\theta = 8\pi

2. Incident Collision Scenarios

- **Projectile Motion and Trajectories**: Use derivatives to determine speed and angles during a collision or vehicle i
  - Position as a function of time s(t)s(t):

v(t)=dsdt,a(t)=dvdt.v(t) = \frac{ds}{dt}, \quad a(t) = \frac{dv}{dt}.

Example: If s(t)=5t2+2ts(t) = 5t^2 + 2t, calculate velocity and acceleration:

1. Velocity:

v(t)=dsdt=10t+2.v(t) = \frac{ds}{dt} = 10t + 2.

2. Acceleration:

a(t)=dvdt=10 m/s2.a(t) = \frac{dv}{dt} = 10 \, \text{m/s}^2.

3. Patrol Research and Route Optimization

- **Travel Path Optimization Using Integrals**: Minimize distance covered by patrol cars along a curve y=f(x)y = f(x
  - Total patrol distance:

L=∫ab1+(dydx)2 dx.L = \int_a^b \sqrt{1 + \left(\frac{dy}{dx}\right)^2} \, dx.

Example: If y=x2y = x^2 and xx ranges from 0 to 1:

1. Compute dydx=2x\frac{dy}{dx} = 2x, so:

L=∫011+(2x)2 dx=∫011+4x2 dx.L = \int_0^1 \sqrt{1 + (2x)^2} \, dx = \int_0^1 \sqrt{1 + 4x^2} \, dx.

2. Approximate using numerical methods.

4. Traffic Management: Collision Impact

- **Impulse and Momentum**: Impulse II is calculated as the integral of force over time:

I=∫t1t2F(t) dt.I = \int_{t_1}^{t_2} F(t) \, dt.

Example: For F(t)=10t2F(t) = 10t^2 from t=0t = 0 to t=3t = 3:

1. Compute:

\[I = \int_0^3 10t^2 \, dt = \left[\frac{10t^{3}}{3}\right]_0^3 = 90 \, \text{Ns}. \]

5. Investigation Principles

- **Decay of Evidence Using Exponential Models**: Biological or chemical evidence decays over time, modeled by:

C(t)=C0e−λt,C(t) = C_0 e^{-\lambda t},

where λ\lambda is the decay rate.

Example: For C0=100 ngC_0 = 100 \, \text{ng}, λ=0.05 day−1\lambda = 0.05 \, \text{day}^{-1}, find C(t)C(t) after 10 days:

1. Compute:

C(10)=100e−0.05·10=100e−0.5≈60.65 ng.C(10) = 100 e^{-0.05 \cdot 10} = 100 e^{-0.5} \approx 60.65 \, \text{ng}.

6. Firearm Ballistics

- **Trajectory Calculations**: The path of a bullet can be calculated using physics and derivatives:
  - Horizontal range:

$$R = \frac{v_0^2 \sin 2\theta}{g},$$

where v_0: initial velocity, θ: angle, $g = 9.8 \, \text{m/s}^2$.

Example: If $v_0 = 300 \, \text{m/s}$ and $\theta = 45^\circ$:

1. Range:

$$R = \frac{300^2 \sin 90^\circ}{9.8} = \frac{90000}{9.8} \approx 9183.67 \, \text{m}.$$

7. Community Policing and Predictive Analysis

- **Crime Trend Analysis Using Regression**: Predict future crimes based on historical data:

$$y = mx + b,$$

where m is the crime trend rate, and b is the baseline.

Example: Given $m = 0.05 \, \text{crimes/day}$ and $b = 10$:

1. Future crime count after 30 days:

$y = 0.05 \cdot 30 + 10 = 11.5 \text{ crimes}.$

These applications highlight the role of calculus in solving real-world policing challenges, from optimizing patrol routes to a **puting**, **information systems**, **computer architecture**, **IT networks**, and **trading systems**, equipping learners with foundat

Column1	Column2	Column3	Column4	Column5

POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY PREPARED BY

THE POL ICING PROJECT AT NYU SCHOOL OF LAW

T A B L E O F C O N T E N T S

INTRO.....01

I.

POLICY AND TRAINING.....02

Create a written policy

Train officers on this policy

II.

FORCE AND SURVEILLANCE.....03

Restrict use of force

Avoid an unnecessarily militarized

presence or aggressive response

Ban mass surveillance

III.

Implement crowd management plans

Develop protocols for officer wellness

Conduct outreach to organizers,

informal leaders, and participants

ADVANCED PLANNING.....05

IV.

ISSUE SPOTLIGHT.....06

Demonstrations about policing

DURING THE EVENT.....07

Respond proportionally

Target enforcement

Communicate transparently

(internally and externally)

V.

AFTER THE EVENT.....12

Evaluate

Re-train

Support

VI.

This report was written by Policing Project Staff

Attorney Katie Kinsey with extensive research and

support from Policing Project 2019-2020 Fellow Julian

Clark. The author wishes to acknowledge the

foundational work of the Police Executive Research Forum

and Edward R. Maguire & Megan Oakley of the Center

for Violence Prevention and Community Safety at Arizona

State University in collaboration with the Harry Frank

Guggenheim Foundation, on which this report builds.

©Policing Project at New York University School of Law

Acknowledgement s :

CONCLUSION.....12

VII.

ISSUE SPOTLIGHT.....09

INTRO.....01

I.

POLICY AND TRAINING.....02

Create a written policy

Train officers on this policy

II.

FORCE AND SURVEILLANCE.....03

Restrict use of force

Avoid an unnecessarily militarized

presence or aggressive response

Ban mass surveillance

III.

Implement crowd management plans

Develop protocols for officer wellness

Conduct outreach to organizers,

informal leaders, and participants

ADVANCED PLANNING.....05

IV.

ISSUE SPOTLIGHT.....06

Demonstrations about policing

DURING THE EVENT.....07

Respond proportionally

Target enforcement

Communicate transparently

(internally and externally)

V.

AFTER THE EVENT.....12

Evaluate

Re-train

Support

VI.

This report was written by Policing Project Staff

Attorney Katie Kinsey with extensive research and

support from Policing Project 2019-2020 Fellow Julian

Clark. The author wishes to acknowledge the

foundational work of the Police Executive Research Forum

and Edward R. Maguire & Megan Oakley of the Center

for Violence Prevention and Community Safety at Arizona

State University in collaboration with the Harry Frank

Guggenheim Foundation, on which this report builds.

©Policing Project at New York University School of Law

Acknowledgement s :

CONCLUSION.....12

VII.

ISSUE SPOTLIGHT.....09

Index

Project goal performamce			
-Indicator correctness descriptive geo map			
-Target			
-Deployment			

-Long life cycle unity			
-Docket system			
Zip TiesINTRO			
The right to engage in peaceful demonstration			
is a cornerstone of American democracy. Yet			

sometimes police fail to strike the right balance,			
approaching demonstrations as a threat to			
public safety, rather than as an expression of			
constitutionally protected rights. This results in			

bad outcomes, for protestors and for police.			
This detailed guide provides an overview of how			
to police demonstrations to protect public			
safety and democratic freedoms. Drawn largely			

from what policing leaders themselves have			
identified as best practices as well as evidence			
based research, it provides clear guidance to			
the police, and informs the public of what they			
should expect. A brief guide summarizing the			

key takeaways discussed here is also available.			
But first, an important caveat: any agency's			
ability to successfully facilitate and de-escalate			
a demonstration will depend in large part on the			

relationship it has with the public before the			
event. Put simply, if an agency hasn't earned the			
public's trust with its everyday policing, it will			
struggle to de-escalate situations during a			
protest—even if it adheres to many of these best			

practices. We say this not to dissuade any			
agencies from implementing these strategies			
during a protest, but rather to emphasize the			
need to practice these principles consistently.			

[1] See generally POLICE EXEC. RESEARCH FORUM, The POLICE RESPONSE TO MASS			
DEMONSTRATIONS:			
PROMISING			
PRACTICES			
AND			
LESSONS			
LEARNED			
(2018),			

https://bit.ly/3egHuPT [hereinafter PERF 2018 REPORT]; EDWARD R. MAGUIRE & MEGAN			
OAKLEY, POLICING PROTESTS—LESSONS FROM THE OCCUPY MOVEMENT, FERGUSON &			

BEYOND: A GUIDE FOR POLICE, https://www.hfg.org/Policing%20Protests.pdf			
[hereinafter POLICING PROTESTS].			
[2] Maggie Koerth & Jamiles Lartey, De-escalation Keeps Protesters and Police Safer.			

Departments Respond with Force Anyway, FIVETHIRTYEIGHT, https://53eig.ht/31PCdJR			
(“Former law-enforcement officials also said good policing of demonstrations isn’t as			

simple as just showing up with an a approachable demeanor. 'The time to make friends			
isn’t when you need them...You have to be in front of it.'").			
Photo by Nathan Dumlao on Unsplash An explicit statement that all police action at			

protests has two, equal goals: upholding the public's First Amendment rights and protecting public safety; Defined key terms so that officers and the			

public understand when and how certain			
provisions of the policy are triggered;			
Detailed procedures for how the agency will			
operationalize its response approach;			
A ban on mass surveillance of protestors;			

Stringent restrictions on the use of force,			
acknowledging that even minor uses of			
unnecessary force may chill rights;			
Specific provisions addressing vulnerable			
populations, such as people with disabilities,			
transgender			

or			
gender			
nonconforming			
individuals, and minors;			
1. Create a written policy for demonstrations			
Agencies should develop a mass demonstrations			
policy that emphasizes free expression, public			

safety, and de-escalation.[3] This policy should			
incorporate public input on key concerns and			
insight from experts on policing, civil liberties,			
and human rights. In general, all agency policies			

should include the following provisions:			
An outline of the parameters and protections			
afforded journalists and legal observers,			
including the conditions under which they must			
be allowed to observe or monitor police			

conduct.			
Education: Instruct officers on their role as the			
facilitators and protectors of peaceful			
demonstrations.			
Emphasize			
constitutional			
rights and adherence to principles of			

procedural justice. Consider partnering with			
journalists and First Amendment legal experts			
to develop training modules on safeguarding			
journalists' and legal observers' rights at			
demonstrations. In addition, training modules			

should review the latest science on crowd			
psychology, which explains that crowds are			
not uniform and that officers are competing			
with agitators for protestors' good will.[4]			

De-escalation: Emphasize the importance of			
de-escalation tactics specific to the protest			
context, including strategies for handling			
antagonistic interpersonal interactions with			

large groups. Use scenario-based training to simulate high-stress protest environments.			
2. Train officers on this policy Following policy reform, training should be modified so that all officers are aware of the			

policy requirements. Key elements of training			
should include:			
POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			
Policy & Training			

[3] E.g., OAKLAND POLICE DEP'T, OAKLAND POLICE DEP'T CROWD CONTROL AND MGMT. POLICY 1 (2013), https://bit.ly/31PMqGk [hereinafter OAKLAND POLICY].			
[4] POLICING PROTESTS, supra note 1 at 49-50.			

02Impact Weapons (i.e. batons): A baton or			
similar device may be authorized for use in a			
non-striking defensive capacity or to stop or			
neutralize a perceived threatening resistance			
(e.g., used in the two-hand horizontal thrust on			

a police line).[5] Impact weapons should not be			
used for general crowd control, containment,			
or dispersal.[6] Intentional baton strikes to the			
head, neck, throat, left armpit or clavicle are			

considered deadly force and may only be used			
when deadly force is authorized.[7] Officers			
should be trained to avoid those areas of the			
body when using a baton.			
3. Restrict Use of Force			

Ensure that use of force is authorized only when			
there is a clear risk to personal safety or to restrain			
acts of property destruction or looting. Whenever			
reasonably possible, officers should give a verbal			

warning prior to any use of force. If authorized,			
officers must use only the minimum amount of			
force necessary and proportionate to de-escalate			
the situation. Once the situation is under control,			
officers who use force immediately should			

administer aid (if trained to do so) or request			
Emergency Medical Services (EMS).			
In addition, policy and practice should include			
clear restrictions on the use of impact weapons			

and chemical weapons, and should prohibit the			
use of distraction devices or impact projectiles to			
disperse crowds. Specifically:			
Pepper Spray: Pepper spray only may be			
used			
proportionately			
against			

specific			
individuals actively resisting arrest, or as			
necessary in a defensive capacity.[8] It should			
not be used on people who are passively			
resisting,			
nor			
should			
it			
be			
sprayed			

indiscriminately over a large area as a means of crowd control.			
Firearms: when safe and feasible, officers should try to de-escalate situations, issue verbal warnings, or use non-lethal force with			

the goal of resolving encounters without using			
deadly force.[9] Firearms almost never should			
be			
unholstered			
or			
used			
during			
a			
demonstration. Officers may use a firearm			

only when they reasonably believe such action			
is			
immediately			
necessary			
to			
protect			
themselves or another person from imminent			
danger of death or serious bodily harm.[10]			

Vehicles: Officers should be prohibited from intentionally creating contact between their vehicles and protestors.[11] Intentional use of a vehicle at any speed to strike a protestor is considered deadly force.[12] Officers also			

should not drive through a demonstration area			
to reach a mobilization point or staging area.			
Helicopters: Helicopters should never be flown			
at low altitudes as a crowd dispersal tactic.			

POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			

[5] INT'L ASS'N OF CHIEFS OF POLICE, IACP MODEL POLICY: CROWD MANAGEMENT 6 (2019), https://bit.ly/37PZG1o [hereinafter IACP MODEL POLICY].			
[6] OAKLAND POLICY, supra note 3, at 13.			

[7] LOUISVILLE METRO POLICE DEP'T, LOUISVILLE METRO POLICE DEP'T STANDARD OPERATING PROCEDURES § 9.1.12, https://bit.ly/35Le8VX.			
[8] IACP MODEL POLICY, supra note 5, at 6.			

[9] CAMDEN CTY. POLICE DEP'T, USE OF FORCE POLICY CORE PRINCIPLE #4, https://bit.ly/2HC0c89			
[10] Id.			

[11]CITY OF PORTLAND OR., PORTLAND POLICE DEP'T DIRECTIVE 635.10, § 10.4 https://bit.ly/35NL7Jg (“Motor bikes or motorcycles shall not be driven into a crowd or used to make physical contact with			
persons.”).			

[12] OAKLAND POLICY , supra note 3, at 15; TUCSON POLICE DEP'T, TUCSON POLICE DEP'T GEN. OPERATING PROCEDURES 2000, § 2080, https://bit.ly/3oxdV0V			

Response plans should start "soft" with officers

wearing regular uniforms and engaging the			
crowd while avoiding formations like lines or			
wedges. Demonstrate a commitment to			
facilitation by providing water or distributing			
face masks to protestors.			

All use of force incidents should be documented			
and reported. Accurately tracking and reporting			
officer-involved force incidents is critical to			
effectively managing a policing agency and			

maintaining the public's trust. Admittedly, the			
potentially chaotic atmosphere of a protest			
presents significant challenges for documenting			
these incidents. Agencies should consider whether			

innovative options may be available to facilitate			
documentation. For example, agencies can require			
officers to report all uses of force live on police			
radio to ensure contemporaneous reporting or			

enable officers to report force incidents in a digital			
log on their agency smartphones. These live			
reporting methods provide a more efficient and			
user-friendly way to capture and track force			
incident data.			

4. Avoid an unnecessarily militarized			
presence or aggressive response			
Use tiered response plans that increase the level of			
engagement in proportion only to actual—not			
assumed or forecasted—conditions on the ground:			

Ensure that officers have ready access to			
helmets if needed to protect themselves			
from head injuries from projectiles or debris.			
Deploy officers in “hard” riot gear as a last			
resort, and only when necessary to protect			

the public or officers from violence or serious			
injury. In case of a violent outbreak, tactical			
units may be staged nearby but out of sight			
of protestors to avoid escalating a peaceful			
crowd.			
5. Ban the mass surveillance of protestors			

Police surveillance of protestors has a chilling			
effect on the constitutionally protected right to			
peacefully assemble. As such, agencies should			
ban the mass surveillance of protestors,			
particularly			
the			

use			
of			
controversial			
technologies, including facial recognition and			
social media surveillance. Use of drones or other			
aerial surveillance should be restricted to			

identifying specific outbreaks of violence or			
looting to enable targeted enforcement. Video			
feeds should not be recorded or stored. If			
protest activities are captured through existing			

surveillance systems, agencies should ensure that			
any resulting images or data are purged after a			
reasonable time period unless necessary to a			
felony investigation.			

Force & Surveillance 6. Implement crowd management plans			
Early and comprehensive planning is essential to			
manage			
protests			
safely			
and			
effectively.			
Developing a clear strategy beforehand allows			

for informed and competent decision making			
during an event.[13] Although today's protests are			
often spontaneous and lack clear leaders,			
agencies still can prepare and train with general			

strategies and operational procedures that will			
guide the response to these flash events.			
When agencies receive advance notice of a			
protest, incident commanders (ICs) should			
prepare tailored, written plans that clearly			

communicate a strategy of facilitation and articulate officers' specific roles and responsibilities.[14] Plans should include education on the likely crowd subgroups and the issues			

behind the protest so that officers can			
understand and communicate with crowd			
members more effectively. They also should			
contemplate			
the			
need			
for			
inter-agency			

coordination prior to or during an event. For example, police may want to partner with the local sanitation agency to remove potential projectile or unintended barrier objects, such as trash cans or dumpsters, from demonstration			

sites.[15]			
To address spontaneous events, ICs should			
prepare generic plans that cover different types			
and sizes of demonstrations to provide generally			
applicable strategic and tactical working			
principles.			
Operational			

plans			
should			
be			
distributed to all officers assigned to an event.[16]			
7. Develop protocols for officer wellness			
Written protocols should be prepared to address			
officers' physical and mental health needs during			

an event. This may include ensuring regular shift			
changes, arranging for adequate rest and			
hydration, and providing face masks.[17] In addition,			
officers should receive specific preparation for the			

verbal assault they may encounter at protests, with			
mental health counseling provided for officers			
subject to traumatic interactions with protestors.			
8. Conduct outreach to organizers, informal			

leaders, and participants			
Agencies should conduct outreach to organizers of			
planned demonstrations or influential participants			
in spontaneous events identified through public			

sources, such as social media. Through this			
outreach, agencies should seek to facilitate			
cooperation and negotiate rules of engagement,			
including what type of behavior will result in what			

level of enforcement action. Police should			
approach these negotiations with a willingness to			
find a middle ground, rather than an expectation			
that all their demands must be met. Any			

negotiated terms should be communicated to the			
broader public through regular and social media.			
For informal protests or when event leaders are			
unwilling to meet with command staff in advance,			

agencies should publicize their rules of engagement			
via press conferences and social media to set clear			
expectations. Regardless of the response to their			
outreach, the police goal must remain to facilitate			

peaceful protest and protect public safety.			
POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			
Advance Planning			

[13] TONY NARR ET AL., POLICE EXEC. RESEARCH FORUM, POLICE MANAGEMENT OF MASS DEMONSTRATIONS: IDENTIFYING ISSUES AND SUCCESSFUL APPROACHES 7 (2006), https://bit.ly/3ozG87s

[14] IACP MODEL POLICY, supra note 5, at 2; THE SEATTLE POLICE DEP'T, THE SEATTLE POLICE DEP'T AFTER ACTION REPORT 52 (2000), https://bit.ly/3kDaPX1			
[15] PERF 2018 REPORT, supra note 1, at 27.			

[16] IACP MODEL POLICY, supra note 5, at 2.			
[17] PERF 2018 REPORT, supra note 1, at 26–27.			

[18] Id. at 78; POLICING PROTESTS, supra note 1, at 68-69; HUNTON & WILLIAMS, FINAL REPORT: INDEP. REVIEW OF THE 2017 PROTEST EVENTS IN CHARLOTTESVILLE, VIRGINIA 8 (2017),			
https://bit.ly/3kBHCeR			

05In general, policing protests about police does not			
require a separate set of best practices from policing			
other protests. Undoubtedly, this context presents			
unique challenges in planning and facilitation. For			

example, protest organizers may be less receptive to			
negotiating terms with police in advance, and			
protestors may display more antagonism toward			
officers.[19] Because of these exact challenges, police			

must adhere even more stringently to the basic best			
practices set forth in this guide: commitment to			
facilitation			
and			
targeted			
enforcement.[20]			
These			
strategies			
promote			
de-escalation			

and			
create			
opportunities to humanize officers in the eyes of			
protestors. Some additional strategies specific to a			
protest about policing include:			
Dialogue Officers or Intermediary Officials: Consider			

using specially trained and attired officers (unarmed,			
casual clothing,			
reflective vests) to serve as			
intermediaries between command and protestors.[21]			
Alternately, consider partnering with other local			

agencies or community or civil rights groups to serve in			
this intermediary role and help manage demonstrations			
when significant animosity toward police is anticipated.			
Officer wellness: Demonstrations that target policing			

itself typically result in increased tensions and			
provocations from protestors. Crowd management			
plans for these demonstrations should provide for			
officers to be rotated out more frequently so they can			

rest, have a meal or a snack, and compose themselves			
before resuming their duties.[22]			
ISSUE SPOTLIGHT:			
PROTESTS ABOUT POLICING			
6			

[19] PERF 2018 REPORT, supra note 1, at 1; POLICING PROTESTS, supra note 1, at 68–69.			
[20] PERF 2018 REPORT, supra note 1, at iii (“Ensuring that police responses to mass demonstrations are			

proportional to the actions and mood of the crowd is critically important. These considerations are			
particularly important for demonstrations that are about police use of force or other police actions, as			

opposed to economic or social issues.”); Berkeley Police Dep’t, Response to Civil Unrest: A Review of			
Berkeley Police Dep’t's Actions & Events of Dec. 6 and 7, 2014 at 49-50 https://bit.ly/37LgUgt			

("Opportunities for the police to use crowd management rather than control tactics should be recognized			
and seized...Perhaps because this protest was about confronting the police to redress grievances against			

‘the police,’ crowd control tactics such as skirmish lines were particularly antagonistic to many in the			
crowd.").			
[21] Similar to the “Community Network Team” model employed by Tucson Police Department. Tucson Police			

Dep’t, Critical Incident Review Board: Congress St./ Granada Ave. Immigration Protest 54–55 (2017),			
https://bit.ly/31S500u (discussing the creation of the “Community Network Team,” whose members are			

“specially selected and trained to deploy during large events and protests.”). See also POLICING			
PROTESTS, supra note 1, at 71.			

[22] POLICING PROTESTS, supra note 1, at 80; see also PERF 2018 REPORT, supra note 1, at 12.9. Respond proportionally			
During a protest, police action always should seek			
to de-escalate—not elevate—tensions with crowd			

members. Whenever possible, agencies should			
avoid an unnecessarily militarized presence or			
aggressive response. To enable this proportional			
approach, use tiered response plans that increase			

the level of engagement in proportion only to			
actual—not assumed or forecasted—conditions on			
the ground. Response plans should start "soft,"			
with officers wearing regular uniforms and			

attempting to engage with the crowd. At this			
stage, any formations that signal the police may			
be preparing to disperse the crowd, such as lines			
or wedges, should be avoided. Officers can			

demonstrate a commitment to facilitation by			
distributing water or face masks to protestors.			
Of course, protests that start peacefully may not			
remain that way, and officer safety is a critical			

concern. If officers are initially deployed in soft			
gear, ensure they have ready access to helmets in			
the event they need to quickly protect themselves			
from head injuries from projectiles or debris. If			

actual violence or property destruction is			
occurring or imminent and officers require			
additional protective gear, agencies may deploy			
bicycle officers as the next phase of a tiered			

response.[23] Bikes provide multiple benefits: they			
are easier to maneuver through a crowd than			
vehicles; officers on bikes are more approachable			
than those in riot gear; and bike helmets provide			

protection without appearing militaristic.[24]			
The final stage of a tiered response plan allows			
for officers to deploy in "hard" gear, like riot gear.			
This stage should be considered a last resort,			
authorized only when necessary to protect the			

public or officers from violence or serious injury. In			
case of a violent outbreak, tactical units may be			
staged nearby, but should remain out of sight of			
protestors to avoid escalating a peaceful crowd. If			

a police force is committed to and trained in the			
principles of de-escalation and facilitation, then			
the need to increase the level of the response			
should be the exception rather than the rule.			
10. Target enforcement			

Along with tiered response plans, agencies should			
target enforcement only to those engaging in			
violence, property destruction, or other serious			
crimes. At large protests, taking police action			

against individuals without affecting peaceful			
bystanders will be difficult, and interventions must			
be well-focused and carefully considered. Even			
when enforcement is necessary against particular			

individuals, officers should continue to facilitate			
peaceful protest. Because of the real potential for			
enforcement to escalate a situation, two			
considerations should guide every enforcement			
decision:			

• The likelihood that police action will improve the			
situation; and			
• The seriousness of the offense(s) and the			
objective dangers they present.			
To implement this approach, instruct and train			

officers to distinguish between violent criminal			
behavior			
and			
lower-level			
acts			
of			
civil			
disobedience. Explain that this strategy requires			
allowing some illegal but nonviolent behavior to			

persist, such as some traffic law violations. It also			
may require issuing citations instead of arrests for			
POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			

During the Event			
[23] PERF 2018 REPORT, supra note 1, at 3.			
[24] Id. at 71.			
07POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			

a broader swath of offenses than typically may			
be permitted.[25] Of course, the decision to issue			
citations for an arrest-eligible offense needs to			
be balanced against legitimate concerns that			

individuals will re-engage in the same illegal			
activity.[26] Yet policing agencies should make a			
concerted effort to use the least restrictive			
enforcement option at the outset and not			
assume, without an articulable basis, that the			

criminal behavior will continue.[27]			
Mass Arrests: Mass arrests should be avoided			
at all costs – they escalate tensions with			
protestors and deplete officer resources at the			
scene.[28] In the rare circumstances in which mass			

arrests may be necessary, incident commanders			
should develop a plan that estimates the number			
of anticipated arrests and ensures sufficient			
staffing.[29] For spontaneous events, the incident			

commander(s) should assess the scene on the			
ground to determine if additional personnel and			
resources are required.[30]			
To enable efficient processing, agencies may			
need to modify their typical arrest procedures to			

expedite processing. For example, agencies can			
develop a shortened intake form or eliminate			
fingerprinting for non-felony offenses.[31] Reducing the the number of			

people			
fingerprinted			
during			
a			
protest			
assumes			
heightened relevance during COVID-19 because			
of public health concerns around shared, high			

contact surfaces. If it is necessary to obtain			
fingerprints, i.e., when booking someone who's			
committed a felony, agencies may consider			
using mobile fingerprint technology to expedite			
the process.[32]			

Agencies also should develop a high-volume			
processing system that prepares certain district			
houses or mobile facilities with adequate			
resources to process arrests as quickly as			
possible.[33] Individuals subject to arrest should			

be brought to the nearest processing facility.[34]			
Transport to a distant location should occur only			
when there is a substantial risk that on-site			
processing would allow the unlawful behavior to			

continue.[35] During processing, precautions			
should be taken to ensure that protestors'			
constitutional rights are respected, including			
providing reasonable access to restrooms,			

water, food, and necessary medical attention.[36]			
Special care should be taken to ensure that			
vulnerable populations, such as people with			
disabilities or transgender individuals, are			

searched and detained in a respectful manner;			
all effort must be made to provide shelter and			
restroom facilities appropriate to their needs			
and identities.			
Crowd Containment: Indiscriminate crowd			

containment measures should rarely, if ever, be			
used; containment without a point of egress			
should never be permitted. Instead, agencies			
should focus on providing clear, well-spaced			
dispersal orders and isolating actual bad actors			

through a targeted enforcement approach.			
Policing agencies should develop a procedure			

[25] See, e.g., OAKLAND POLICY, supra note 3, at 19 (recommending citation and release for minor offenses rather than custodial arrest); cf. COVID-19: Stay-At-Home and Social Distancing Enforcement,			

POLICING PROJECT, https://bit.ly/3jJ8RDi (last updated May 20, 2020) (“Agencies are encouraged to avoid custodial arrests absent offenses that involve imminent public safety threats such as harm to			

others, and instead approach infractions through education and awareness. Even issuing citations should be considered carefully given the catastrophic financial impact of the pandemic on many			

individuals and families.”); Police Responses to COVID-19, Brennan Center, https://bit.ly/3kPd3lW (last updated July 8, 2020) (recommending police "issue warnings whenever possible. In the case of more			

severe infractions, police should issue a summons or a ticket in lieu of making an arrest absent an immediate threat to public safety.").			
[26] OAKLAND POLICY, supra note 3, at 20.			
[27] Id.			

[28] POLICE EXEC. RESEARCH FORUM, MANAGING MAJOR EVENTS: BEST PRACTICES FROM THE FIELD 44 (2011).			
[29] OAKLAND POLICY, supra note 3 at 19.			

[30] E.g., CHICAGO POLICE DEP'T, MASS ARREST PROCEDURES SPECIAL ORDER S06-6 at III.A https://bit.ly/2TxArIP (Sept.27, 2018).

[31] Id.

[32] Mobile Fingerprint Identification, P.A. CHIEFS POLICE ASS'N, https://bit.ly/2HHEuA0 [hereinafter MOBILE FINGERPRINT IDENTIFICATION]; U.S. DEP'T HOMELAND SEC., MOBILE IDENTIFICATION			

FINGERPRINT DEVICES MARKET SURVEY REPORT 1-3 (January 2015), https://bit.ly/3kCglJf; VERA INSTITUTE OF JUSTICE, LOS ANGELES COUNTY JAIL OVERCROWDING REDUCTION PROJECT FINAL			

REPORT 18 (Sept. 2011), https://bit.ly/34CUJHc; Memorandum from Danielle M. Outlaw (Mar. 17, 2020), https://bit.ly/2HGO5Ha.			
[33] PERF 2018 Report, supra note 1, at 18.			

[34] OAKLAND POLICY, supra note 3, at 19 (requiring that arrestees be cited "at or near the demonstration cite" or, in the alternative, from "temporary processing stations or police facilities as near the site of arrest as possible.").

[35] Id.

[36] See id. (requiring that detained arrestees receive “reasonable access to toilet facilities and to appropriate medical attention”).			
08Zip-ties—also known as flex cuffs—are lightweight hand			
restraints made of plastic or nylon that are ar			

economical, disposable alternative to traditional metal			
handcuffs.[37] Unlike metal handcuffs, zip ties do not lock			
into a single fixed position when placed on a person’s			
wrists.[38] Because of their low cost and light weight, they			

often are used by police to make a large number of			
arrests in a dynamic situation.[39] Yet, their flexibility also			
can lead to injury as the cuffs can continue to tighten			
after they're placed on an individual's wrists.[40] Excessive			

tightening and improper use of zip-tie cuffs can cause			
serious pain, bruising, lacerations, and numbness—or even			
permanent nerve damage.[41]			
Because of these known risks, agencies instead should			

consider alternative restraint options, such as tri-fold			
disposable restraints.[42] Made of plastic and designed for			
use by law enforcement, tri-fold restraints can lock in a			
fitted position on a person’s wrist and thus reduce the			

potential for excessive tightening and subsequent injury.[43]			
Require that officers carry flex cutters with them			
whenever they might use zip-tie cuffs.[44]			
Require officers applying zip-ties to write their badge			

number in permanent marker on the cuffs so that			
supervisors or protestors can hold officers accountable			
for cuffs that are used improperly or maliciously.[45]			
Explicitly require that arrestees in flex cuffs are			

checked at regular intervals, such as every 15 minutes,			
to ensure proper fit. [46]			
Although these handcuffs may be more expensive than			
zip-ties, they still are more economical and more practical			
for field use than traditional metal handcuffs.			

Agencies that are unwilling or unable to procure tri-fold			
restraints can reduce the risks posed by zip ties by			
adopting the following best practices:			
ISSUE SPOTLIGHT: ZIP TIES			
CONSIDER ALTERNATIVES, OR RESTRICT THEIR USE			

[37] SARAH KNUCKEY, KATHERINE GLENN, EMI MACLEAN, ET AL., SUPPRESSING PROTEST: HUMAN RIGHTS VIOLATIONS IN THE U.S. RESPONSE TO OCCUPY WALL ST. 78 (2012), https://bit.ly/2Ja609z

[hereinafter SUPPRESSING PROTEST].

[38]See, e.g., Gerry McNeilly, POLICING THE RIGHT TO PROTEST: G20 SYSTEMIC REVIEW REPORT, OFFICE OF THE INDEPENDENT POLICE REVIEW DIRECTOR 238, https://bit.ly/34Bb3Im; (May 2012) [hereinafter McNeilly].

[39] Id.

[40] Id.

[41] See also, Peter Senzamici, Plastic Handcuff Use by NYPD During Anti-Brutality Protests Strikes a Nerve, CITY, https://bit.ly/37OmSwV [hereinafter SENZAMICI].			

[42] Tri-Fold Restraints, ASP, https://bit.ly/3jCYUab (last visited Aug. 7, 2020).			

[43]See McNeilly, supra note 39, at 238-39 (noting that tri-fold restraints, such as the ASP plastic wrist restraint, "can be locked . . . to reduce the potential for the restraint to tighten and cause unnecessary pain or injury to the detainee").			

[44] See, e.g., OAKLAND POLICY supra note 3 at 19 (“each unit involved in detention and/or transportation of arrestees with flex-cuffs should have a flex-cuff cutter and adequate supplies of extra flex			

cuffs readily available.”); Sacramento Police Department, Search & Handcuff Manual, 4 https://bit.ly/34zeTBT (“Officers using flex cuffs must have a cutting tool in their possession in order to remove the			

cuffs. A wire cutter or diagonal cutter should be used rather than a knife.”).			
[45] OAKLAND POLICY, supra note 3, at 19.			

[46] SUPRESSING PROTEST supra note 37 at 44 (quoting Nevada Dep't. of Corr. Admin. Reg. 407, Use of Handcuffs and Restraints 3).			
[47] PERF 2018 REPORT, supra note 1, at 27; IACP MODEL POLICY, supra note 5, at 5.			

[48] IACP MODEL POLICY, supra note 5, at 5; PERF 2018 REPORT, supra note 1, at 27; POLICING PROTESTS, supra note 1, at 78–79 (“provide people with the opportunity to ‘heed the warnings and exit the area’”).

[49] IACP MODEL POLICY, supra note 5, at 5.			
[50] PERF 2018 REPORT, supra note 1, at 27.			
for communicating warnings to protestors prior to			
dispersing crowds. This should cover the time and			

manner in which warnings are given and how many			
times warnings will be repeated before arrests			
occur.[47] Warnings must be clearly audible and			
should consist of the offense or violations being			

committed that necessitate dispersal.[48] Agencies			
may need to invest in adequate loudspeakers			
and/or station officers at different ends of the			
crowd to ensure all affected protesters can hear			

warnings. Long range acoustic devices may be			
used as public address systems, but they should not			
be deployed as a crowd control or dispersal tactic.			
Names of officers issuing dispersal orders should			

be recorded in the command log.[49] If police have			
sufficient notice of demonstrations, they should			
communicate these procedures and expectations			
to the public beforehand.[50] In addition, officers			

POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			
THE POLICING PROJECT AT NYU LAW			
09POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			

THE POLICING PROJECT AT NYU LAW			
Exit: Officers should never encircle a crowd			
without providing a consistent point of exit.[55]			
should be trained in the procedures for crowd			
containment tactics, including simulations during			

scenario-based training.			
Police should avoid kettling, or other restrictive containment tactics, unless absolutely necessary.[51] Kettling is a crowd control tactic in			

which police confine a group of demonstrators in			
a small area and control access in and out of the			
area. In limited situations, targeted crowd			
containment practices may serve to de-escalate			

potentially violent situations while avoiding police			
use of force.[52] For example, police may attempt			
to separate and contain actually violent members			
of a crowd as an alternative to arrest or using			

force and/or to prevent a breach of peace from			
expanding. Still, kettling or any containment			
practice that doesn’t provide exit points or			
differentiate peaceful protestors raises legitimate			

legal and human rights concerns.[53] Adopting a			
targeted approach to protest policing should			
obviate the need to deploy group containment			
tactics.[54]			
In the limited situations in which large-scale			

crowd containment measures are necessary,			
agencies should apply the following best			
practices:			
Communication:			
Clear warnings, in multiple languages,			
should be issued prior to implementing any			

containment tactic with real opportunity to comply.[56]			
Officers should never encircle a crowd and subsequently order them to disperse.[57]			
Officers should provide regular updates to contained individuals on duration and			

reasons for containment.[58]			
Differentiation:			
Agency policy and guidelines should include a general prohibition on containing media and legal observers.[59]			
All efforts should be made to contain only violent			

protestors,			
with			
non-violent			
protestors and bystanders identified and			
allowed to filter out as soon as possible.[60]			
Welfare:			
Care should be rendered to anyone			

experiencing a medical emergency in the containment zone.[61]			
Discomfort of those contained should be limited, with plans in place to provide access to toilets and water.[62]			
Duration: Containment should last only as long			

as is absolutely necessary to quell violence or			
risk of serious injury to non-violent protestors			
and bystanders.[63]			

[51] NAT'l POLICING IMPROVEMENT AGENCY, MANUAL OF GUIDANCE ON KEEPING THE PEACE 110 (2010) https://bit.ly/31NGP31 [hereinafter NPIA REPORT]; see also Use of Police Lines, D.C. Code § 5-			

331.08 (2005) https://bit.ly/3jKXuuB (prohibiting the encirclement of protestors except in limited circumstances such as to ensure demonstrators' safety); European Court Says 'Kettling' Tactics in 2001			

Lawful, BBC (March 15, 2012), https://bbc.in/3jGX7Rn (reporting European Court of Human Rights' decision that kettling may be lawful if deployed in particular circumstances and to protect human life			
and avoid property damage).			

[52] PORTLAND CITY AUDITOR, POLICY REVIEW: POLICE BUREAU CAN IMPROVE ITS APPROACH TO CROWD CONTROL DURING ST. PROTESTS 9 (2018), https://bit.ly/34zx22A [hereinafter PORTLAND			
POLICY REVIEW].			

[53] POLICING PROTESTS, supra note 1, at 76; PERF 2018 REPORT, supra note 1, at 73.			
[54] POLICING PROTESTS, supra note 1, at 76			
[55] PERF 2018 REPORT, supra note 1, at 19, 73.			

[56] NPIA REPORT, supra note 51, at 110; cf. PERF 2018 REPORT, supra note 1, at 72; IACP MODEL POLICY, supra note 5, at 4–5 (recommending clear warnings given prior to arrests or forced crowd dispersal);			

PORTLAND POLICY REVIEW, supra note 52, at 12 (recommending a policy on mass detentions that includes warnings provided to protestors prior to detention).			
[57] PERF 2018 REPORT, supra note 1, at 27.			

[58] NPIA REPORT, supra note 51, at 110.[5]			
[59] PORTLAND POLICY REVIEW, supra note 52, at 12.			

[60] NPIA REPORT, supra note 51, at 110; see also, POLICING PROTESTS, supra note 1, at 76 (condemning overly restrictive crowd containment measures and recommending a differentiated response strategy			

that targets only those actually engaged in criminal activity).			
[61] NPIA REPORT, supra note 51, at 111.			
[62] Id.; PORTLAND POLICE REVIEW, supra note 52, at 12.			

[63] See NPIA Report, supra note 51, at 110 (directing that crowd containment tactics be limited in time).

11. Communicate transparently (both internally and externally)			
During a protest, clear communication reduces conflict and promotes safety for officers and protestors alike. Internally, officers should have			

access to a dedicated radio line for logistics and			
to communicate needs to command for essentials			
like food, water, or medical attention.			
Policing agencies also should develop external			

communication plans for protestors, the general			
public,			
and			
the			
media.			
Agencies			
should			
acknowledge the essential roles played by			
journalists and legal observers and ensure their			

access to information and ability to do their jobs			
unobstructed			
absent			
serious			
public			
safety			
concerns. Legal observers should have access to			
areas where arrests are being made unless their			

presence			
would			
in			
fact			
obstruct			
lawful			
enforcement action. Even then, visual access for			
media and legal observers should be preserved.			

To reduce the administrative burden on police and			
remove any appearance of a conflict of interest,			
press credentialing and legal observer registration			
should be handled by a separate agency or neutral			

body. Agencies also should consider maintaining			
an agency press officer in the field to answer			
journalists' questions and address issues raised.			
To communicate with demonstrators, agencies			

should ensure that all announcements or warnings			
are audible and well documented. Agencies should			
implement a clear warning procedure, discussed			
above, that			
requires			
multiple, well-spaced			

warnings in relevant languages before any			
enforcement action.[64] To inform the general public,			
agencies			
should			
share			
live			
updates			
and			
information on social media during the course of			

an event. For multi-day protests, agencies also			
should share live updates and information on social			
media during the course of an event. For multi-day			
protests, agencies also should conduct daily press			

conferences that share rules of engagement,			
enforcement rationale, and accurate information			
while correcting misinformation.[65]			
Command should share intelligence with protest			

leaders about outside agitators infiltrating lawfully			
planned protests and demonstrations. Certainly,			
that information will affect the policing agencies'			
strategy and their operations before and during			
the demonstration. It is plausible that such			

information also may impact protest leaders' plans,			
communications and safety measures. In the spirit			
of facilitating peaceful protests and protecting			
those who choose to exercise their First			
Amendment rights, agencies should do everything			

in their power to ensure peaceful and lawful			
demonstrations are not thwarted by those with			
ulterior motives. To not share such pertinent			
information not only jeopardizes the demonstration			

and its orderliness but it also jeopardizes the safety			
of the event’s participants.			
Relatedly officers should never attempt to covertly			
infiltrate a group engaged in protest activities			

unless there is reasonable suspicion that the group			
is planning to engage in criminal activity and there			
are no less intrusive investigatory means.			
Undercover police activity at protests can chill First			

Amendment rights and lead to violence.[66]			
Finally, officer anonymity should be prohibited, with			
badges and nameplates clearly visible at all times.			
As David Couper, the former Madison, Wisconsin			
Chief of Police and a noted expert in protest			

policing has explained, "[a]nonymity or any			
depersonalization of police conducting crowd			
management			
encourages			
negative			
crowd			
behavior. It can also lead to unaccountable			

behavior on the part of the police."[67] If displaying			
names			
presents			
demonstrated			
harassment			
concerns, officers should be clearly identified with			
numbers. Similarly, police leadership should be			

visible, with on-the-ground command staff			
available to respond to issues raised by protestors.			
[64] Koerth & Lartey, supra note 2 (describing transparent communication as a best practice de-escalation tactic).			

[65] PERF 2018 REPORT, supra note 1, at 58, 79.			
[66] Sahil Singhvi, Police Infiltration of Protests Undermines the First Amendment, BRENNAN CENTER (Aug. 4, 2020), https://bit.ly/34AqC36			

[67] David Couper, Crowds, Protest and Police, Improving Police, Oct. 31, 2011, https://bit.ly/34Cjxiz.			
1112. Evaluate			
Some of the most important policing work begins			
when a protest ends in the form of internal			

evaluation. For larger demonstrations or those that			
result in violence or uses of force, policing agencies			
should engage in comprehensive after-action			
reviews to understand what went right and what			
could be improved. Ideally, these reports should be			

conducted by a neutral party, such as an Inspector			
General. They should include investigations of all			
uses of force and should contain feedback from			
event organizers, participants, and other affected			

community members to ensure the review			
represents a holistic picture of the event. All			
findings should be made public.			
13. Retrain			
Following these reviews and at regular intervals,			

demonstration training should be re-evaluated			
and updated to reflect lessons learned from			
post-event assessments.			
14. Support			
Finally, officers should be provided with access			

to counseling and peer support as needed in			
the event of violence or other traumatic or			
stressful events during a protest.			
POLICING PROTESTS TO PROTECT CONSTITUTIONAL RIGHTS AND PUBLIC SAFETY			

After the Event

Conclusion

Protests present some of the most complex and challenging situations police face. This guide

provides strategic and operational recommendations to enable fair and effective policing practices			
before, during, and after these events. Implementing these recommendations should help ensure that			

an agency's approach to protest policing not only protects public safety but also preserves citizens'			
constitutional rights.			
For more information on the Policing Project, visit PolicingProject.org			

ISC2 Security Congress Submission Notification

Inbox

noreply@gocadmium.com

Mon, May 5, 5:51 PM (9 days ago)

to me, tshingombekb

Dear tshingombe tshingombe,

ISC2 would like to thank you for the time and effort you spent on submitting a proposal for ISC2 Security Congress 2025. We were fortunate to have many strong proposals to choose from, but only a limited number could be selected. Unfortunately, we are unable to accept your submission, "thesis master engineering Thesis master doctoral engineering electrical subject ciriculum framework qualicafition Education technology," at this time.

We received more than 600 proposals this year for 80 available speaking slots, so there were many quality submissions that did not get selected. Submissions went through a lengthy review and rating process involving more than 30 experienced cybersecurity practitioners and subject matter experts. Please note that, given the large volume of submissions, we are unable to provide any further information on why your submission was not accepted.

Again, we thank you for your effort and interest. ISC2 and the Security Congress team appreciate your continued support.

Sincerely,

Bradley Barth

Global Event Program Manager

ISC2 Events Team

bbarth@isc.org

LAST CHANCE: Register for the AI & Cybers Skills Webinar!

Inbox

ISACA <isaca@em.isaca.org> Fri, May 9, 8:42 AM (5 days ago)

Unsubscribe

to me

Webinar

AI & Cyber Skills: Audit, Manage, and Analyze

Learn about ISACA's new advanced AI credentialing program that builds on existing expertise and a cybersecurity analyst program featuring performancebased labs to validate handson experience. Join us to discover how ISACA® can support your AI and cyber skill development and help you earn valuable new credentials.

Webinar Speakers

Safia Kazi, AIGP, CIPT

Principal, Privacy Professional Practices

ISACA

When: 13 May 2023 |

Times: 8 am CT / 13 pm CT / 6 pm CT |

(Can't join live? View ondemand until 13 May 2026)

Register Now

ISACA

1700 East Golf Road Suite 400, Schaumburg,
IL, 60173, US

Web Version | Manage Email Preferences |
ISACA Privacy Notice

INTAIEM1R0425

© 2025 ISACA. All rights reserved.

ISACA <isaca@em.isaca.org>

Fri, May 9, 12:06 AM (5 days ago)

Unsubscribe

to me

Dear Tshingombe,

Understanding and implementing digital trust has never been easy. But the new DTEF platform makes it a little easier. The reimagined DTEF combines content, tools and Focus Areas into a single, seamless experience. So your efforts are more productive and more effective than ever.

Digital tools

Digital tools have been integrated into the content, for easier, more intuitive access to resources.

Focus Areas

Focus Areas have been added to help with adoption and implementation.

Realtime content updates

Realtime content updates provide easy access to the most current information, guidelines and tools. No new editions to downlo

Questions about the M.A. in Public Policy degree?

Inbox

Coursera	Thu, May 8, 8:45 AM (6 days ago)
Unsubscribe	

to me

Get your questions answered today!

Are you wondering about the application process? Want to know if you can try a course before enrolling? Read our FAQ about the M.A. in Public Policy and get answers about career paths, tuition payments, and more. Then, you can feel more ready to apply!

Apply now

Frequently asked questions
1. Is the degree flexible?

As a learner, you will have the flexibility to go through the pre-recorded videos, readings, and practice questions entirely at your own pace. Approximately, 10 hours of weekly commitment will be required.

2. What are the career outcomes?

As an Masters in Public Policy graduate, you will be equipped to work in development and public policy organisations, CSR initiatives, academic institutions, think tanks, NGOs, media, and political organizations.

3. What appears on the degree? Is it the same as an on-campus degree?

Students who complete the programme will earn a master's degree. This degree will be the same as an on-campus degree. (No mention of online in the degree title). However, online mode of learning will be mentioned on the back side of the certificate, as per the guidelines of the University Grants Commission, Govt. of India.

You have received this message because you have expressed interest in a degree program.

Help

Follow

Coursera for Business

Email Settings

Unsubscribe

Privacy Notice

© 2025 Coursera Inc. All rights reserved. Coursera and the Coursera logo are registered trademarks of Coursera, Inc. All other trademarks are property of their respective owners. Log in to manage all your notification preferences in Email Settings.

Coursera | 2440 W El Camino Real 5th floor, Mountain View, CA 94040 USA

- d Bartlett Learning. (Sep, 2020).

- Building an Information Security Awareness Program, 1st Ed. by Bill Gardner and Valerie Thomas. Publisher: Syngr

- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syr

- Cybersecurity Risk Management by Cynthia Brumfield, Brian Haugli. Publisher: Wiley. (Dec, 2021).

- Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).

- Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Jar

- Distributed Denial of Service (DDoS) by Eric Chou, Rich Groves. Publisher: O'Reilly Media, Inc. (Apr, 2018).

- Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock.

- Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bart

- Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, 1st Ed. by Corey

- Information Security Policies, Procedures, and Standards: A Practitioner's Reference by Dogulas J. Landoll. Publish

· ISC2 Code of Ethics by ISC2. (Dec, 2023).

- Mastering Windows Security and Hardening by Mark Dunkerley, Matt Tumbarello. Publisher: Packt Publishing. (Au
- Modern Cryptography for Security Professionals, 1st Ed. by Lisa Bock. Publisher: Packt Publishing. (Jun, 2021).
- Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlet
- Networking Fundamentals, 1st Ed. by Gordon Davies. Publisher: Packt Publishing. (Dec, 2019).
- Network Security Strategies by Aditya Mukherjee. Publisher: Packt Publishing. (Nov, 2020).
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Kar
- Security Policies and Implementation Issues, 3rd Ed. by Robert Johnson and Chuck Easttom. Publisher: Bartlett Lea

- The Complete Guide to Physical Security by Paul R. Baker and Daniel J. Benny. Publisher: Auerbach Publications. (A
- A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, D

- Access Control and Identity Management, 3rd Ed. by Mike Chapple. Publisher: Jones and Bartlett Learning. (Sep, 2

- A Technical Guide to IPSec Virtual Private Networks by James S. Tiller. Publisher: Auerbach Publications. (Jul, 2017

- Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publis

- Building an Information Security Awareness Program, 1st Ed. by Bill Gardner and Valerie Thomas. Publisher: Syngr

- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syn

- Cryptography and Network Security Principles and Practice, 6th Ed. by William Stallings. Publisher: Pearson. (Mar,

- Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents by Eric C. Thompson. Pul

- Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).
- Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock.
- Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bart
- Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution by Darran Rolls, Mor
- Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmar
- Information Risk Management: A Practitioner's Guide by David Sutton. Publisher: BCS, The Chartered Institute for
- Introduction to Computer Networks and Cybersecurity, 1st Ed. by J. Chwan-Hwa Wu, David Irwin. Publisher: CRC P

· ISC2 Code of Ethics by ISC2. (Dec, 2023).

- Logging and Log Management by A. Chuvakin, K. Schmidt. Publisher: Syngress. (Dec, 2012).

- Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlet

- Networking Fundamentals, 1st Ed. by Gordon Davies. Publisher: Packt Publishing. (Dec, 2019).

- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Kar

- Official (ISC)² SSCP CBK Reference, 5th Ed. by Mike Wills. Publisher: Sybex. (Dec, 2019).

- Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (M
- A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, D

- Access Control, Authentication, and Public Key Infrastructure (Information Systems Security & Assurance), 1st Ed.

- Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O'Reilly Media, Inc.

- Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) by Michael Ka
- Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations by Morey J.
- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syr
- Computer and Information Security Handbook, 3rd Ed. by John Vacca. Publisher: Morgan Kaufmann. (May, 2017).
- Computer Security: Art and Science, 2nd Ed. by Matt Bishop. Publisher: Addison-Wesley Professional. (Nov, 2018)
- Core Software Security: Security at the Source by Anmol Misra, James F. Ransome. Publisher: Auerbach Publicatio
- Data Center Handbook, 2nd Ed. by Hwaiyu Geng. Publisher: Wiley. (May, 2021).
- Developing Cybersecurity Programs and Policies, 3rd Ed. by Omar Santos, Sari Greene. Publisher: Pearson IT Certif
- Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Jar

- Distributed Denial of Service (DDoS) by Eric Chou, Rich Groves. Publisher: O'Reilly Media, Inc. (Apr, 2018).
- DomainKeys Identified Mail (DKIM) Signature by Murray Kucherawy, Dave Crocker, Tony Hansen. Publisher: IETF. (
- Ethical Hacking and Penetration Testing Guide by Rafay Baloch. Publisher: Auerbach Publications. (Sep, 2017).
- Federated Identity Primer, 1st Ed. by Derrick Rountree. Publisher: Syngress. (Dec, 2012).
- Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock.
- Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle P
- Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bart
- EU General Data Protection Regulation (GDPR) by European Parliament. Publisher: European Parliament and Cour

- Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmar

- Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution by Darran Rolls, Mor

- Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, 1st Ed. by Corey

- Information Security Handbook by Darren Death. Publisher: Packt Publishing. (Dec, 2017).

- Information Security Policies, Procedures, and Standards: A Practitioner's Reference by Dogulas J. Landoll. Publish

- Introduction to Computer Networks and Cybersecurity, 1st Ed. by J. Chwan-Hwa Wu, David Irwin. Publisher: CRC P

· ISC2 Code of Ethics by ISC2. (Dec, 2023).

- IT Auditing Using Controls to Protect Information Assets, 3rd Edition by Mike Kegerreis, Mike Schiller, Chris Davis.

- Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlet
- Network Vulnerability Assessment: Identify Security Loopholes in Your Network's Infrastructure by Sagar Rahalkar
- Networking Fundamentals, 3rd Ed. by Chuck Easttom, Richard M. Roberts. Publisher: Goodheart-Willcox. (Sep, 20
- NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep,
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Paulin
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy by Karen Scarfone, Paul Hoffman. (Sep, 200
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc
- NIST SP 800-63-3, Digital Identity Guidelines: Enrollment and Identity Proofing by Paul A. Grassi, James L. Fenton, I
- NIST SP 800-77, Revision 1, Guide to IPsec VPNs by Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, Pau

- NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin S
- NIST SP 800-95, Guide to Secure Web Services by Anoop Singhal, Theodore Winograd, Karen Scarfone. (Aug, 2007
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Sc
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) by Erika McCal
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems by Arnold Johnsc
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organiz
- NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engi
- Official (ISC)² Guide to the CISSP CBK, 5th Ed. by John Warsinske, Mark Graff, Kevin Henry, Christopher Hoover, Be

- OWASP Testing Guide, Release 4.0 by Matteo Meucci, Andrew Muller. Publisher: OWASP. (Dec, 2014).
- Physical Security and Safety by Jeffrey Dingle, Bobby E. Ricks, Truett A, Ricks. Publisher: CRC Press. (Oct, 2014).
- Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (M
- Practical Internet of Things Security, 2nd Ed. by Brian Russel, Drew Van Duren. Publisher: Packt Publisher. (Nov, 20
- Securing Open Source Libraries by Guy Podjarny. Publisher: O'Reilly Media, Inc. (Nov, 2017).
- Securing VoIP, 1st Ed. by Regis Bates. Publisher: Syngress. (Nov, 2014).
- Security Policies and Implementation Issues, 3rd Ed. by Robert Johnson and Chuck Easttom. Publisher: Bartlett Lea
- Security Risk Assessment: Managing Physical and Operational Security by John M. White. Publisher: Butterworth-H

- Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0 by
- The Complete Guide to Physical Security by Paul R. Baker and Daniel J. Benny. Publisher: Auerbach Publications. (A
- The Disaster Recovery Handbook, 3rd Ed. by Michael Wallace, Lawrence Webber. Publisher: AMACOM. (Dec, 201
- Threat Modeling: Designing for Security, 1st Ed. by Adam Shostack. Publisher: Wiley. (Feb, 2014).
- Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman. P
- Zero Trust Networks: Building Secure Systems in Untrusted Networks by Evan Gilman, Doug Barth. Publisher: O'Re
- Architecting Cloud Computing Solutions by Kevin L. Jackson and Scott Goessling. Publisher: Packt Publishing. (May
- Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) by Michael Ka
- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syn

- Cloud Computing Design Patterns by Thomas Erl, Robert Cope, Amin Naserpour. Publisher: Prentice Hall. (Mar, 20
- Cloud Security Handbook by Eyal Estrin. Publisher: Packt Publishing. (Apr, 2022).
- Data Governance: The Definitive Guide by Evren Eryurek, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Gran
- EU General Data Protection Regulation (GDPR) by European Parliament. Publisher: European Parliament and Cour
- Fundamental Practices for Secure Software Development. Publisher: SAFECode. (Mar, 2018).
- Guide to Privacy and Security of Electronic Health Information. Publisher: HealthIT.gov. (Apr, 2015).
- Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incid
- Information Security Handbook by Darren Death. Publisher: Packt Publishing. (Dec, 2017).

- NIST SP 800-125, Guide to Security for Full Virtualization Technologies by Karen Scarfone, Murugiah Souppaya, Pa

- Official (ISC)² Guide to the CCSP CBK, 3rd Ed. by Leslie Fife, Aaron Kraus, Bryan Lewis. Publisher: Sybex. (July, 2021

- Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (M

- Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 by Rich Mogull, James Arlen, Adrian Lane, G

- Security, Privacy, and Digital Forensics in the Cloud by Lei Chen, Hassan Takabi, Nhien-An Le-Khac. Publisher: Wile
- Information Security Risk Management for ISO 27001/ISO 27002, 3rd Ed. by Alan Calder, Steve Watkins. Publisher

- ISO 27001/ISO 27002, A Pocket Guide, 2nd Ed. By Alan Calder. Publisher: IT Governance Publishing. (Oct, 2013).

- NIST FIPS-199, Standards for Security Categorization of Federal Information and Information Systems by U.S. Dept

- NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems by Marianne Swanso

- NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep,
- NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc
- NIST SP 800-53A, Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations by Join
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations by Joint Task Force Transformation
- NIST SP 800-60, Vol. 1, Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categ
- NIST SP 800-70, Rev. 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
- NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin S

- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organiz
- A Guide to Building Secure Web Applications and Web Services 2.0 Black Hat Ed. by Abraham Kang, Adrian Wiesm
- A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, D
- Access Control, Authentication, and Public Key Infrastructure, 2nd Ed. by Mike Chapple, Bill Ballad, Tricia Ballad, Er
- Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O'Reilly Media, Inc.
- Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publis
- CMMI for Development: Implementation Guide by Mukund Chaudhary, Abhishek Chopra. Publisher: Apress. (Dec,
- Computer Security: Art and Science, 2nd Ed. by Matt Bishop. Publisher: Addison-Wesley Professional. (Nov, 2018)
- Core Software Security: Security at the Source by Anmol Misra, James F. Ransome. Publisher: Auerbach Publicatio

- Cybersecurity - Attack and Defense Strategies, 2nd Ed. by Erdal Ozkaya and Yuri Diogenes. Publisher: Packt Publish
- Enterprise Software Security: A Confluence of Disciplines by Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Dia
- Hacker Techniques, Tools, and Incident Handling, 2nd Ed. by Sean-Philip Oriyano. Publisher: Jones & Bartlett Learr
- Hands-On Security in DevOps by Tony Hsu. Publisher: Packt Publishing. (Jul, 2018).
- Improper Error Handling by Jeremy Ferragamo, Wichers, Jim Bird. Publisher: OWASP. (Dec, 2021).
- Information Security: Principles and Practices, 2nd Ed. by Mark S. Merkow, Jim Breithaupt. Publisher: Pearson IT C
- IT Release Management: A Hands-on Guide by Dave Howard. Publisher: CRC Press. (Apr, 2016).
- IT Security Risk Control Management: An Audit Preparation Plan by Raymond Pompon. Publisher: Apress. (Sep, 20

- Lessons Learned in Software Testing: A Context-Driven Approach by Bret Pettichord, Cem Kaner, James Marcus Ba
- Logging and Log Management by A. Chuvakin, K. Schmidt. Publisher: Syngress. (Dec, 2012).
- Mastering the Requirements Process: Getting Requirements Right v3.0 by S. Robertson, J. Robertson. Publisher: A
- NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cy
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc
- NIST SP 800-60, Vol. 1, Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categ
- NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin S
- NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems by Jon Boyens, C

- Official (ISC)² Guide to the CSSLP, 2nd Ed. by Mano Paul. Publisher: Auerbach Publications. (Aug, 2013).
- OWASP Testing Guide, Release 4.0 by Matteo Meucci, Andrew Muller. Publisher: OWASP. (Dec, 2014).
- Penetration Testing: A Survival Guide by W. Halton, B. Weaver, J. Ansari, S. Kotipalli, M. Imran. Publisher: Packt Pu
- Security Risk Management by Evan Wheeler. Publisher: Syngress. (Apr, 2011).
- Software Testing Foundations: A Study Guide for the Certified Tester Exam, 4th Ed. by Andreas Spillner. Publisher:
- Web Application Firewalls by Chad Russell. Publisher: O'Reilly Media, Inc. (Apr, 2018).
- Agile Application Lifecycle Management: Using DevOps to Drive Process Improvement, 1st Ed. by Bob Aiello, Leslie
- Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O'Reilly Media, Inc.
- Architecting Secure Software Systems, 1st Ed. by Asoke Talukder, Manish Chaitanya. Publisher: Auerbach Publicati

- Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publis
- Beginning Database Design Solutions by Rod Stephens. Publisher: Jossey-Bass. (Nov, 2008).
- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syr
- Cloud Storage Security: A Practical Guide by Aaron Wheeler, Michael Winburn. Publisher: Elsevier. (Jul, 2015).
- Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev. 5 by Mead, N. Publisher: Carneg
- Data Center Handbook, 2nd Ed. by Hwaiyu Geng. Publisher: Wiley. (May, 2021).
- Disaster Recovery and Business Continuity, 3rd Ed. by B.S. Thejandra. Publisher: IT Governance Publishing. (Jan, 20
- Enterprise Security Architecture: A Business-Driven Approach, 1st Ed. by John Sherwood. Publisher: CRC Press. (No

- Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmar
- Information Security Management Handbook, Vol. 6, 6th Ed. by Harold F. Tipton and Micki Krause Nozaki. Publishe
- Information Security Management Handbook, Vol. 7, 6th Ed. by Richard O'Hanley, James Tiller. Publisher: Auerbac
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Paulin
- NIST SP 800-57, Rev. 5, Recommendation for Key Management: Part 1 – General by Elaine Barker. Publisher: NIST.
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Kar
- NIST SP 800-63-3, Digital Identity Guidelines: Enrollment and Identity Proofing by Paul A. Grassi, James L. Fenton, I
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Sc
-]NIST SP 800-125, Guide to Security for Full Virtualization Technologies by Karen Scarfone, Murugiah Souppaya, Pa

- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations by Vincent Hu, Da
- Official (ISC)² Guide to the ISSAP CBK, 2nd Ed. by Adam Gordon. Publisher: Auerbach Publications. (Jan, 2017).
- Payment Card Industry Data Security Standards, Requirements and Security Assessment Procedures, Version 3.2.1
- Practical Internet of Things Security, 2nd Ed. by Brian Russel, Drew Van Duren. Publisher: Packt Publisher. (Nov, 20
- SABSA Executive Summary by SABSA. Publisher: The SABSA Institute. (Dec, 2021).
- Secure Coding in C and C++, 2nd Ed. by Robert Seacord. Publisher: Addison-Wesley Professional. (Apr, 2013).
- Security Patterns in Practice: Designing Secure Architectures Using Software Patterns by Eduardo Fernandez-Bugli
- Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 by Rich Mogull, James Arlen, Adrian Lane, G
- A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th Ed. by Project Management Institute

- INCOSE Systems Engineering Handbook by Walden. Publisher: Wiley. (Jul, 2015).
- Information Assurance Technical Framework 3.1 by National Security Agency Information Assurance Solutions Tec
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation by ISO/IEC. Publisher: National Inf
- NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep,
- NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint
- NIST SP 800-40, Rev. 3, Guide to Enterprise Patch Management Technologies Murugiah Souppaya, Karen Scarfone
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc

- NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin S
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Sc
- NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engi
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information System and Organizations by Jo
- A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th Ed. by Project Management Institute
- Auditing IT Infrastructures for Compliance, 2nd Ed. by Martin Weiss. Publisher: Jones & Bartlett Publishers. (Jul, 20
- Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syn
- Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).
- Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Jan

•□Disaster Recovery Planning: For Computers and Communication Resources by Jon Toigo. Publisher: Wiley. (Jan, 19

•□Information Security Management Handbook, Vol. 6, 6th Ed. by Harold F. Tipton and Micki Krause Nozaki. Publishe

· ISC2 Code of Ethics by ISC2. (Dec, 2023).

•□Incident Response & Computer Forensics, 3rd Ed. by Jason Luttgens, Matthew Pepe, Kevin Mandia. Publisher: Mc

•□IT Auditing Using Controls to Protect Information Assets, 3rd Edition by Mike Kegerreis, Mike Schiller, Chris Davis.

•□NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep,

•□NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Paulin

•□NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cy

- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Forc
- NIST SP 800-55, Rev. 1, Performance Measurement Guide for Information Security by Elizabeth Chew, Marianne S
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Kar
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems by Arnold Johnsc
- NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engi
- Official (ISC)² Guide to the ISSMP CBK by Joseph Steinberg and Harold F. Tipton. Publisher: Auerbach Publications.
- Security Operations Center: Building, Operating, and Maintaining your SOC by Gary McIntyre, Joseph Muniz, Nadh
- The Disaster Recovery Handbook, 3rd Ed. by Michael Wallace, Lawrence Webber. Publisher: AMACOM. (Dec, 201

- Threat Modeling: Designing for Security, 1st Ed. by Adam Shostack. Publisher: Wiley. (Feb, 2014).

nline Training

Official ISC2 Certified in Cybersecurity (CC) eTextbook

eTextbook Description

< Return to Listing

The Official ISC2 Certified in Cybersecurity (CC) eTextbook is your go-to learning resource as you prepare for the CC exam. It

Price: $24.95

Language:

English

Japanese

Who Should Purchase:

IT professionals, career-changers, college students, recent graduates and executives seeking foundational knowledge in cyb

What to Expect:

A comprehensive review of the Official ISC2 Training Course content related to the ISC2 Certified in Cybersecurity exam. Lea

· Chapter overviews, objectives and summaries

· Informative graphics

· Key terms and definitions

· Chapter quizzes and answer keys

CPE Credits

None

Access Period:

365 days from inital access

This eTextbook covers the following:

Chapter 1: Security Principles

- 1: Understand the Security Concepts of Information Assurance
- 2: Understand the Risk Management Process
- 3: Understand Security Controls
- 4: Understand Governance Elements and Processes

- 5: Understand ISC2 Code of Ethics

Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts

- 1: Understand Incident Response
- 2: Understand Business Continuity
- 3: Understand Disaster Recovery

Chapter 3: Access Controls Concepts

- 1: Understand Access Control Concepts
- 2: Understand Physical Access Controls
- 3: Understand Logical Access Controls

Chapter 4: Network Security

- 1: Understand Computer Networking
- 2: Understand Network (Cyber) Threats and Attacks
- 3: Understand Network Security Infrastructure

Chapter 5: Security Operations

- 1: Understand Data Security
- 2: Understand System Hardening
- 3: Understand Best Practice Security Policies
- 4: Understand Security Awareness Training

Technology Requirements:

The CC eTextbook uses VitalSource eReader, which will allow you to view materials on multiple devices and platforms, onlin

The following may be among system requirements to access your eTextbook.

- A stable and continuous internet connection.

Hardware Specifications

- Processor 2 GHz +

- RAM 4 GB +
- Monitor minimum resolution (1024 x 768)
- Video Card
- Keyboard and Mouse or other assistive technology

Supported Operating Systems

- Macintosh OS X 10.10 to present
- Windows 10 to present

Supported Browsers

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Application Software

- VitalSource eReader
- Certification Exam Outline
- Effective Date: November 15, 2022
- ISSMP Certification Exam Outline
- About CISSP-ISSMP
- The Information Systems Security Management Professional (ISSMP) is a CISSP who specializes in establishing,
- presenting and governing information security programs and demonstrates management and leadership
- skills. CISSP-ISSMPs direct the alignment of security programs with the organization’s mission, goals and
- strategies in order to meet enterprise financial and operational requirements in support of its desired risk
- position.
- The broad spectrum of topics included in the CISSP-ISSMP Common Body of Knowledge (CBK®) ensure its
- relevancy across all disciplines in the field of information security management. Successful candidates are
- competent in the following six domains:
- Leadership and Business Management
- Systems Lifecycle Management
- Risk Management
- Threat Intelligence and Incident Management

- • Contingency Management
- • Law, Ethics and Security Compliance Management
- Experience Requirements
- Candidates must be a CISSP in good standing and have two years cumulative paid work experience
- in one or more of the six domains of the CISSP-ISSMP CBK. You can learn more about CISSP-ISSMP
- experience requirements and how to account for part-time work and internships at
- www.isc2.org/Certifications/CISSP-Concentrations#steps-to-certification.
- Accreditation
- CISSP-ISSMP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.
- Job Task Analysis (JTA)
- (ISC)² has an obligation to its membership to maintain the relevancy of the CISSP-ISSMP. Conducted at
- regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that
- are performed by security professionals who are engaged in the profession defined by the CISSP-ISSMP. The
- results of the JTA are used to update the examination. This process ensures that candidates are tested on the
- topic areas relevant to the roles and responsibilities of today's practicing information security professionals.3
- ISSMP Certification Exam Outline
- CISSP-ISSMP Examination Information
- CISSP-ISSMP Examination Weights
- Length of exam
- Number of items
- Item format
- Passing grade
- Exam availability
- Testing center
- 3 hours
- 125
- Multiple choice
- 700 out of 1000 points
- English
- Pearson VUE Testing Center
- Domains
- Weight

- 1. Leadership and Business Management
- 20%
- 2. Systems Lifecycle Management
- 18%
- 3. Risk Management
- 19%
- 4. Threat Intelligence and Incident Management
- 17%
- 5. Contingency Management
- 15%
- 6. Law, Ethics and Security Compliance Management
- 11%
- **Total: 100%**4
- ISSMP Certification Exam Outline
- **Domain 1:**
- **Leadership and Business Management**
- 1.1 Establish security's role in organizational culture, vision and mission
- » Define information security program vision and mission
- » Align security with organizational goals, objectives and values
- » Define security's relationship to the overall business processes
- » Define the relationship between organizational culture and security
- 1.2 Align security program with organizational governance
- » Identify and navigate organizational governance structure
- » Validate roles of key stakeholders
- » Validate sources and boundaries of authorization
- » Advocate and obtain organizational support for security initiatives
- 1.3 Define and implement information security strategies
- » Identify security requirements from business initiatives
- » Evaluate capacity and capability to implement security strategies
- » Manage implementation of security strategies
- » Review and maintain security strategies
- » Prescribe security architecture and engineering theories, concepts and methods

- 1.4 Define and maintain security policy framework Determine applicable external standards
- » Determine applicable external standards
- » Determine data classification and protection requirements
- » Establish internal policies
- » Advocate and obtain organizational support for policies
- » Develop procedures, standards, guidelines and baselines
- » Ensure periodic review of security policy framework

- » Define roles and responsibilities
- » Determine and manage team accountability
- » Build cross-functional relationships
- » Resolve conflicts between security and
- other stakeholders
- » Identify communication bottlenecks
- and barriers
- » Integrate security controls into human
- resources processes
- » Evaluate service management agreements
- (e.g., risk, financial)
- » Govern managed services
- (e.g., infrastructure, cloud services)
- » Manage impact of organizational change (e.g.,
- mergers and acquisitions, outsourcing)
- » Ensure that appropriate regulatory compliance
- statements and requirements are included in
- contractual agreements
- » Monitor and enforce compliance with
- contractual agreements
- 1.5 Manage security requirements in contracts and agreements
- 1.6 Manage security awareness and training programs
- » Promote security programs to key stakeholders
- » Identify needs and implement training programs by target segment

- » Monitor and report on effectiveness of security awareness and training programs
- 1.7 Define, measure and report security metrics
- » Identify Key Performance Indicators (KPI)
- » Associate Key Performance Indicators (KPI) to the risk posture of the organization
- » Use metrics to drive security program development and operations
- 1.8 Prepare, obtain and administer security budget
- » Prepare and secure annual budget
- » Adjust budget based on evolving risks and threat landscape
- » Manage and report financial responsibilities
- 1.9 Manage security programs
- 1.10 Apply product development and project management principles
- » Incorporate security into project lifecycle
- » Identify and apply appropriate project management methodology
- » Analyze project time, scope and cost relationship6
- ISSMP Certification Exam Outline
- 2.1 Manage integration of security into Systems Development Life Cycle (SDLC)
- » Integrate information security gates (decision points) and requirements into lifecycle
- » Implement security controls into system lifecycle
- » Oversee security configuration management (CM) processes
- 2.2 Integrate new business initiatives and emerging technologies into the
- security architecture
- » Integrate security into new business initiatives and emerging technologies
- » Address impact of new business initiatives on security posture
- 2.3 Define and oversee comprehensive vulnerability management programs
- (e.g., vulnerability scanning, penetration testing, threat analysis)
- » Identify, classify and prioritize assets, systems and services based on criticality to business
- » Prioritize threats and vulnerabilities
- » Manage security testing
- » Manage mitigation and/or remediation of vulnerabilities based on risk
- 2.4 Manage security aspects of change control
- » Integrate security requirements with change control process
- » Identify and coordinate with the stakeholders

- » Manage documentation and tracking
- » Ensure policy compliance (e.g., continuous monitoring)
- Domain 2:
- Systems Lifecycle Management 7
- ISSMP Certification Exam Outline
- Domain 3:
- Risk Management
- 3.1 Develop and manage a risk management program
- » Identify risk management program objectives
- » Communicate and agree on risk management objectives with risk owners and other stakeholders
- » Determine scope of organizational risk program
- » Identify organizational security risk tolerance/appetite
- » Obtain and verify organizational asset inventory
- » Analyze organizational risks
- » Determine countermeasures, compensating and mitigating controls
- » Perform cost-benefit analysis (CBA) of risk treatment options
- 3.2 Conduct risk assessments
- » Identify risk factors
- 3.3 Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk)
- » Identify supply chain security risk requirements
- » Integrate supply chain security risks into organizational risk management
- » Validate security risk control within the supply chain
- » Monitor and review the supply chain security risks3
- ISSMP Certification Exam Outline
- 4.1 Establish and maintain threat intelligence program
- » Aggregate threat data from multiple threat intelligence sources
- » Conduct baseline analysis of network traffic, data and user behavior
- » Detect and analyze anomalous behavior patterns for potential concerns
- » Conduct threat modeling
- » Identify and categorize an attack
- » Correlate related security event and threat data
- » Create actionable alerting to appropriate resources

- 4.2 Establish and maintain incident handling and investigation program
- » Develop program documentation
- » Establish incident response case management process
- » Establish incident response team
- » Apply incident management methodologies
- » Establish and maintain incident handling process
- » Establish and maintain investigation process
- » Quantify and report financial and operational impact of incidents and investigations to stakeholders
- » Conduct root cause analysis (RCA)
- Domain 4:
- Threat Intelligence and Incident
- Management 9
- ISSMP Certification Exam Outline
- 5.1 Facilitate development of contingency plans
- » Identify and analyze factors related to the Continuity of Operations Plan (COOP)
- » Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification)
- » Identify and analyze factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)
- » Coordinate contingency management plans with key stakeholders
- » Define internal and external crisis communications plans
- » Define and communicate contingency roles and responsibilities
- » Identify and analyze contingency impact on business processes and priorities
- » Manage third-party contingency dependencies
- » Prepare security management succession plan
- 5.2 Develop recovery strategies
- » Identify and analyze alternatives
- » Recommend and coordinate recovery strategies
- » Assign recovery roles and responsibilities
- 5.3 Maintain contingency plan, Continuity of Operations Plan (COOP), business continuity
- plan (BCP) and disaster recovery plan (DRP)
- » Plan testing, evaluation and modification
- » Determine survivability and resiliency capabilities
- » Manage plan update process

- 5.4 Manage disaster response and recovery process
- » Declare disaster
- » Implement plan
- » Restore normal operations
- » Gather lessons learned
- » Update plan based on lessons learned
- Domain 5:
- Contingency Management 10
- ISSMP Certification Exam Outline
- 10
- 6.1 Identify the impact of laws and regulations that relate to information security
- 6.2 Adhere to the (ISC)
- 2
- Code of Ethics as related to management issues
- 6.3 Validate compliance in accordance with applicable laws, regulations and industry
- best practices
- 6.4 Coordinate with auditors and regulators in support of the internal and external
- audit processes
- 6.5 Document and manage compliance exceptions
- » Identify and document compensating controls and workarounds
- » Report and obtain authorized approval of risk waiver
- Domain 6:
- Law, Ethics and Security Compliance
- Management
- » Identify applicable privacy laws
- » Identify legal jurisdictions the organization and
- users operate within (e.g., trans-border data flow)
- » Identify export laws
- » Identify intellectual property (IP) laws
- » Identify applicable industry regulations
- » Identify and advise on non-compliance risks
- » Inform and advise senior management

- » Evaluate and select compliance framework(s)
- » Implement the compliance framework(s)
- » Define and monitor compliance metrics
- » Plan
- » Schedule
- » Coordinate audit activities
- » Evaluate and validate findings
- » Formulate response
- » Validate implemented mitigation and
- remediation actions11
- ISSMP Certification Exam Outline
- **Additional Examination Information**
- Supplementary References
- Candidates are encouraged to supplement their education and experience by reviewing
- relevant resources that pertain to the CBK and identifying areas of study that may need
- additional attention.
- View the full list of supplementary references at www.isc2.org/certifications/References.
- Examination Policies and Procedures
- (ISC)2 recommends that CISSP-ISSMP candidates review exam policies and procedures
- prior to registering for the examination. Read the comprehensive breakdown of this
- important information at www.isc2.org/Exams/Before-Your-Exam.
- Legal Info
- For any questions related to (ISC)
- 2
- 's legal policies, please contact the (ISC)2 Legal
- Department at legal@isc2.org.
- Any Questions?
- (ISC)2 Americas
- Tel: +1.866.331.ISC2 (4722)
- Email: info@isc2.org
- (ISC)2 Asia-Pacific
- Tel: +(852) 28506951

- Email: isc2asia@isc2.org
- (ISC)2 EMEA
- Tel: +44 (0)203 300 1625
- Email: info-emea@isc2.org
- 11

v222Register for exam

Effective Date: August 29, 2022

Certified in Cybersecurity Certification Exam Outline

View and download the latest PDF version of the Certified in Cybersecurity Exam Outline in the following languages:

CC - English | CC - Chinese | CC - Japanese | CC - German | CC - Spanish

About Certified in Cybersecurity

ISC2 developed the Certified in Cybersecurity (CC) credential for newcomers to the field, to recognize the growing trend of p

The topics on the CC exam include:

- Security Principles
- Incident Response, Business Continuity (BC) and Disaster Recovery (DR) Concepts
- Access Controls Concepts
- Network Security
- Security Operations

Certified in Cybersecurity Examination Information

Length of exam	2 hours
Number of items	100
Item format	Multiple choice
Passing grade	700 out of 1000 points

Exam language availability	English, Chinese, Japanese, German, Spanish
Testing center	Pearson VUE Testing Center

Certified in Cybersecurity Examination Weights	
Domains	**Average Weight**
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%
3. Access Controls Concepts	22%
4. Network Security	24%

5. Security Operations	18%
Total	**100%**

[Boost your chances of passing the exam with the CC eTextbook]

[Build your fundamental cybersecurity knowledge and prepare for the exam.]

[Get eTextbook]

Domains

1.1 - Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

1.2 - Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment and treatment

1.3 - Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4 - Understand ISC2 Code of Ethics

- Professional code of conduct

1.5 - Understand governance processes

- Policies
- Procedures
- Standards

•□Regulations and laws
2.1 - Understand business continuity (BC)
•□Purpose
•□Importance
•□Components
2.2 - Understand disaster recovery (DR)
•□Purpose
•□Importance
•□Components
2.3 - Understand incident response
•□Purpose
•□Importance
•□Components
3.1 - Understand physical access controls
•□Physical security controls (e.g., badge systems, gate entry, environmental design)
•□Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
•□Authorized versus unauthorized personnel
3.2 - Understand logical access controls
•□Principle of least privilege
•□Segregation of duties
•□Discretionary access control (DAC)
•□Mandatory access control (MAC)
•□Role-based access control (RBAC)
4.1 - Understand computer networking
•□Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/
•□Ports
•□Applications
4.2 - Understand network threats and attacks
•□Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-c
•□Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrus
•□Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))
4.3 - Understand network security infrastructure

- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, f
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private ne
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastru

5.1 - Understand data security

- Encryption (e.g., symmetric, asymmetric, hashing)
- Data handling (e.g., destruction, retention, classification, labeling)
- Logging and monitoring security events

5.2 - Understand system hardening

- Configuration management (e.g., baselines, updates, patches)

5.3 - Understand best practice security policies

- Data handling policy
- Password policy
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policy
- Change management policy (e.g., documentation, approval, rollback)
- Privacy policy

5.4 - Understand security awareness training

- Purpose/concepts (e.g., social engineering, password protection)
- Importance

A safe and secure cyber world

The Center for Cyber Safety & EducationISC2 CareersCommunityBlog

Frequently Asked QuestionsContact UsPolicies and Procedures

ISC2 Authorized China AgencyISC2 Japan

© Copyright 1996-2025. ISC2, Inc. All Rights Reserved.

All contents of this site constitute the property of ISC2, Inc. and may not be copied, reproduced or distributed without prior

Sitemap

Certified in Cybersecurity Exam Outline

Access Period:

365 days from inital access

This eTextbook covers the following:

Chapter 1: Security Principles

- 1: Understand the Security Concepts of Information Assurance
- 2: Understand the Risk Management Process
- 3: Understand Security Controls
- 4: Understand Governance Elements and Processes
- 5: Understand ISC2 Code of Ethics

Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts

- 1: Understand Incident Response
- 2: Understand Business Continuity
- 3: Understand Disaster Recovery

Chapter 3: Access Controls Concepts

- 1: Understand Access Control Concepts
- 2: Understand Physical Access Controls
- 3: Understand Logical Access Controls

Chapter 4: Network Security

- 1: Understand Computer Networking
- 2: Understand Network (Cyber) Threats and Attacks
- 3: Understand Network Security Infrastructure

Chapter 5: Security Operations

- 1: Understand Data Security
- 2: Understand System Hardening
- 3: Understand Best Practice Security Policies
- 4: Understand Security Awareness Training

Technology Requirements:

The CC eTextbook uses VitalSource eReader, which will allow you to view materials on multiple devices and platforms, onlin

The following may be among system requirements to access your eTextbook.

- A stable and continuous internet connection.

Hardware Specifications

- Processor 2 GHz +
- RAM 4 GB +
- Monitor minimum resolution (1024 x 768)
- Video Card
- Keyboard and Mouse or other assistive technology

Supported Operating Systems

- Macintosh OS X 10.10 to present
- Windows 10 to present

Supported Browsers

- Google Chrome

•□• Microsoft Edge
•□• Mozilla Firefox
Application Software
•□VitalSource eReader
Online Training
Continuing education
Stay relevant and on top of the latest trends. Leverage our online courses to gain interactive, engaging and timely learning e
The self-paced learning format delivers modular content combined with interactive activities involving videos, labs, case stu
ISC2; Members and Associates have free unlimited access to coursesthat are denoted as 'Free for Members' by logging in a
For individual course purchases learners will have access to the course content for 180 days from the time of purchase.Ple
For All Access and Express Learning Bundle purchases learners will have access to the course content for 365 day from the
1 2 3 > >|
Certification
Defining the Boundaries of Zero Trust Top of Form
Bottom of Form

This learning experience invites you to review the set of guiding principles for workflow, system design, and operations that create a zero trust architecture. (2.0 CPE)

Top of Form

Bottom of Form

Software Inventory and SBOM

Top of Form

Bottom of Form

This course invites you to expand your knowledge of how Software Bill of Materials (SBOM) can help cybersecurity professionals effectively mitigate vulnerabilities and ensure compliance.

Top of Form

Bottom of Form		
	Software Inventory and SBOM	Top of Form
		Bottom of Form

This course invites you to expand your knowledge of how Software Bill of Materials (SBOM) can help cybersecurity professionals effectively mitigate vulnerabilities and ensure compliance.

Top of Form

Bottom of Form

Working in the Cloud

Top of Form

Bottom of Form

This course invites you to learn about the range of challenges security professionals face as they work to utilize, optimize and secure critical assets in the cloud.

Top of Form

Bottom of Form

Working in the Cloud

Top of Form

Bottom of Form

This course invites you to learn about the range of challenges security professionals face as they work to utilize, optimize and secure critical assets in the cloud.

Top of Form

Bottom of Form

Moving to the Cloud

Top of Form

Bottom of Form

This course invites you to learn about the strategic and security considerations necessary to transition an organization to cloud computing in alignment with business needs.

Top of Form		
Bottom of Form		
	Moving to the Cloud	Top of Form
		Bottom of Form

This course invites you to learn about the strategic and security considerations necessary to transition an organization to cloud computing in alignment with business needs.

Top of Form

Bottom of Form

Cloud Basics

Top of Form

Bottom of Form

This course invites you to learn about essential cloud concepts and principles, including key drivers for use, essential characteristics, and service and deployment models within cloud architectures.

Top of Form		
Bottom of Form		
	Cloud Basics	Top of Form
		Bottom of Form

This course invites you to learn about essential cloud concepts and principles, including key drivers for use, essential characteristics, and service and deployment models within cloud architectures.

Top of Form

Bottom of Form		
	Building Your Personal Brand and Digital Presence	Top of Form
		Bottom of Form

This course invites you to review the essentials of building a personal brand and digital presence that reflects your core values, unique strengths and professional aspirations.

Top of Form

Bottom of Form

Resume/CV/Portfolio Building and Management

Top of Form

Bottom of Form

This course invites you to review the critical components of documents such as resumes, CVs and portfolios that showcase your unique strengths and value to potential employers.

Top of Form
Bottom of Form
Identifying and Building Your Network Top of Form
Bottom of Form

This course invites you to review the critical role networking plays in professional development by unlocking new opportunities, facilitating knowledge sharing and supporting long-term career success.

Top of Form

Bottom of Form

Identifying Your Cyber Path and Industry

Top of Form

Bottom of Form

This course invites you to explore a wide range of opportunities in cybersecurity and plan a skill development path toward a successful career.

Top of Form

Bottom of Form

Nailing the Interview Process

Top of Form

Bottom of Form

This course invites you to review actionable strategies and skills to excel in any interview scenario and stand out from the competition.

Top of Form

Bottom of Form

Managing the Offer and Negotiation Process

Top of Form

Bottom of Form

This course invites you to review the essential knowledge and skills to navigate job offers, negotiate confidently and transition smoothly into new roles.

Top of Form

Bottom of Form

Managing the Offer and Negotiation Process

Top of Form

Bottom of Form

This course invites you to review the essential knowledge and skills to navigate job offers, negotiate confidently and transition smoothly into new roles.

Top of Form

Bottom of Form

[Nailing the Interview Process](#)

Top of Form

Bottom of Form

This course invites you to review actionable strategies and skills to excel in any interview scenario and stand out from the competition.

Top of Form

Bottom of Form

Identifying Your Cyber Path and Industry

Top of Form

Bottom of Form

This course invites you to explore a wide range of opportunities in cybersecurity and plan a skill development path toward a successful career.

Top of Form		
Bottom of Form		
	Identifying and Building Your Network	Top of Form
		Bottom of Form

This course invites you to review the critical role networking plays in professional development by unlocking new opportunities, facilitating knowledge sharing and supporting long-term career success.

Top of Form

Bottom of Form

	Resume/CV/Portfolio Building and Management	Top of Form
		Bottom of Form

This course invites you to review the critical components of documents such as resumes, CVs and portfolios that showcase your unique strengths and value to potential employers.

Top of Form

Bottom of Form

1 2 3 > >|

Top of Form

Bottom of Form

Go to the main content

Privacy and Cookies This website stores cookies on your computer which help us make the website work better for you.

Collapsed, toggle side navigation to expand

Edit my profile Tshingombe Tshingombe Tshitadi
ISC2 ID: 1907033

- · Dashboard
- · My Profile
- •□
- •□
- · Sign out

Top of Form

Bottom of Form

Find an exam

Top of Form

Find an Exam:

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

CC	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Certified in Cybersecurity (CC)" Certified in Cybersecurity (CC)

CCSP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Certified Cloud Security Professional (CCSP)" Certified Cloud Security Professional (CCSP)

CGRC	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Certified in Governance Risk and Compliance" Certified in Governance Risk and Compliance

CISSP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Certified Information Systems Security Professional" Certified Information Systems Security Professional

CSSLP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Certified Secure Software Lifecycle Professional" Certified Secure Software Lifecycle Professional

ISSAP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Information Systems Security Architecture Professional" Information Systems Security Architecture Professional

ISSEP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Information Systems Security Engineering Professional" Information Systems Security Engineering Professional

ISSMP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Information Systems Security Management Professional" Information Systems Security Management Professional

SSCP	href="https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" title="Systems Security Certified Practitioner" Systems Security Certified Practitioner

Bottom of Form

· Terms

· Privacy

· Contact

Copyright 1996-2025 Pearson Education Inc. or its affiliate(s). All rights reserved.

Certification is Just the Beginning

Achieving your certification isn't the end of your journey. ISC2 members and associates are part of a global community of cybersecurity professionals with access to a long list of benefits that include continuing professional education, peer-to-peer networking and exclusive discounts.

Stay focused on your goal and make the most of what's ahead.

Preview Your Benefits

ISC2 625 N Washington Street, Suite 400,
Alexandria, VA 22314, United States •
www.isc2.org

© 1996–2024. ISC2, Inc. All rights reserved.

You're receiving this email because you've expressed interest in Certifications, Education Resources and Offers. Click to unsubscribe, or update your subscription preferences on the Member Website.

Register for exam

Effective Date: September 2024

SSCP Certification Exam Outline

View and download the latest PDF version of the SSCP Certification Exam Outline in the following languages:

SSCP - English | SSCP - Japanese | SSCP - Spanish

About SSCP

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practica

The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all discipli

- Security Concepts and Practices
- Access Controls
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

Experience Requirements

Candidates must have a minimum of one year cumulative work experience in one or more of the domains of the SSCP CBK. A

A candidate that doesn't have the required experience to become an SSCP may become an Associate of ISC2 by successfully passing t

Accreditation

SSCP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the SSCP. Conducted at regular intervals, the Job Task

SSCP Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Language availability	English, Japanese and Spanish
Testing center	Pearson VUE Testing Center

SSCP Examination Weights	
Domains	Average Weight
1. Security Concepts and Practices	16%
2. Access Controls	15%
3. Risk Identification, Monitoring and Analysis	15%
4. Incident Response and Recovery	14%
5. Cryptography	9%
6. Network and Communications Security	16%

7. Systems and Application Security	15%
Total	**100%**
Domains	
1.1 - Comply with codes of ethics	
•□ISC2 Code of Ethics	
•□Organizational code of ethics	
1.2 - Understand security concepts	
•□Confidentiality	
•□Integrity	
•□Availability	
•□Accountability	
•□Non-repudiation	
•□Least privilege	
•□Segregation of duties (SoD)	
1.3 - Identify and implement security controls	
•□Technical controls (e.g., firewalls, intrusion detection systems (IDS), access control list (ACL)	
•□Physical controls (e.g., mantraps, cameras, locks)	
•□Administrative controls (e.g., security policies, standards, procedures, baselines)	
•□Assessing compliance requirements	
•□Periodic audit and review	
1.4 - Document and maintain functional security controls	
•□Deterrent controls	
•□Preventative controls	

•□Detective controls
•□Corrective controls
•□Compensating controls
1.5 - Support and implement asset management lifecycle (i.e., hardware, software, and data)
•□Process, planning, design and initiation
•□Development /Acquisition (e.g., DevSecOps, testing)
•□Inventory and licensing (e.g., open source, closed-source)
•□Implementation/Assessment
•□Operation/Maintenance/End of Life (EOL)
•□Archival and retention requirements
•□Disposal and destruction
1.6 - Support and/or implement change management lifecycle
•□Change management (e.g., roles, responsibilities, processes, communications, audit)
•□Security impact analysis
•□Configuration management (CM)
1.7 - Support and/or implement security awareness and training (e.g., social engineering/phishing/tabletop exercises/awa
1.8 - Collaborate with physical security operations (e.g., data center/facility assessment, badging and visitor management,
2.1 - Implement and maintain authentication methods
•□Single/Multi-factor authentication (MFA)
•□Single sign-on (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID Connect)
•□Device authentication (e.g., certificate, Media Access Control (MAC) address, Trusted Platform Module (TPM))
•□Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))
2.2 - Understand and support internetwork trust architectures
•□Trust relationships (e.g., 1-way, 2-way, transitive, zero)
•□Internet, intranet, extranet, and demilitarized zone (DMZ)
•□Third-party connections (e.g., application programming interface (API), app extensions, middleware)

2.3 - Support and/or implement the identity management lifecycle
•□Authorization
•□Proofing
•□Provisioning/De-provisioning
•□Monitoring, Reporting, and Maintenance (e.g., role changes, new security standards)
•□Entitlement (e.g., inherited rights, resources)
•□Identity and access management (IAM) systems
2.4 - Understand and administer access controls
•□Mandatory
•□Discretionary
•□Role-based (e.g., subject-based, object-based, Privileged Access Management (PAM))
•□Rule-based
•□Attribute-based
3.1 - Understand risk management
•□Risk visibility and reporting (e.g., risk register, sharing threat intelligence, indicators of Compromise (IOC), Commo
•□Risk management concepts (e.g., impact assessments, threat modeling, scope)
•□Risk management frameworks
•□Risk tolerance (e.g., appetite, risk quantification)
•□Risk treatment (e.g., accept, transfer, mitigate, avoid)
3.2 - Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
3.3 - Perform security assessments and vulnerability management activities
•□Risk management frameworks implementation
•□Security testing
•□Risk review (e.g., internal, supplier, architecture)
•□Vulnerability management lifecycle (e.g., scanning, reporting, analysis, remediation)
3.4 - Operate and monitor security platforms (e.g., continuous monitoring)

- Source systems (e.g., applications, security appliances, network devices, hosts)
- Events of interest (e.g., errors, omissions, anomalies, unauthorized changes, compliance violations, policy failures
- Log management (e.g., policy, integrity, preservation, architectures, configuration, aggregation, tuning)
- Security information and event management (SIEM) (e.g., real-time monitoring, analysis, tracking, audit)

3.5 - Analyze monitoring results

- Security baselines and anomalies (e.g., correlation, noise reduction)
- Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)
- Event data analysis
- Document and communicate findings (e.g., escalation)

4.1 - Understand and support incident response lifecycle (e.g., National Institute of Standards and Technology (NIST), Inter

- Preparation (e.g., defining roles, training programs)
- Detection, analysis, and escalation (e.g., incident communication, public relations)
- Containment
- Eradication
- Recovery (e.g., incident documentation)
- Post incident activities (e.g., lessons learned, new countermeasures, continuous improvement)

4.2 - Understand and support forensic investigations

- Legal (e.g., civil, criminal, administrative) and ethical principles
- Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
- Reporting of analysis
- Organization Security Policy Compliance

4.3 - Understand and support business continuity plan (BCP) and disaster recovery plan (DRP)

- Emergency response plans and procedures (e.g., information system contingency, pandemic, natural disaster, cris
- Interim or alternate processing strategies
- Restoration planning (e.g., Restore Time Objective (RTO), Restore Point Objectives (RPO), Maximum Tolerable Dov
- Backup and redundancy implementation
- Testing and drills (e.g., playbook, tabletop, disaster recovery exercises, scheduling)

5.1 - Understand reasons and requirements for cryptography
•□Confidentiality
•□Integrity and authenticity
•□Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health informati
•□Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), Internationa
•□Cryptography entropy (e.g., quantum cryptography, quantum key distribution)
5.2 - Apply cryptography concepts
•□Hashing
•□Salting
•□Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC)
•□Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trai
•□Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (R
•□Cryptographic attacks and cryptanalysis
5.3 - Understand and implement secure protocols
•□Services and protocols
•□Common use cases (e.g., credit card processing, file transfer, web client, virtual private network (VPN), transmissi
•□Limitations and vulnerabilities
5.4 - Understand public key infrastructure (PKI)
•□Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange,
•□Web of Trust (WOT) (e.g., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)
6.1 - Understand and apply fundamental concepts of networking
•□Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
•□Network topologies
•□Network relationships (e.g., peer-to-peer (P2P), client server)
•□Transmission media types (e.g., wired, wireless)
•□Software-defined networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization,
•□Commonly used ports and protocols

6.2 - Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name Sys
•□Countermeasures (e.g., content delivery networks (CDN), firewalls, network access controls, intrusion detection a
6.3 - Manage network access controls
•□Network access controls, standards and protocols (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.
•□Remote access operation and configuration (e.g., thin client, virtual private network (VPN), virtual desktop infrastr
6.4 - Manage network security
•□Logical and physical placement of network devices (e.g., inline, passive, virtual)
•□Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL)
•□Secure device management
6.5 - Operate and configure network-based security appliances and services
•□Firewalls and proxies (e.g., filtering methods, web application firewall (WAF), cloud access security broker (CASB))
•□Network intrusion detection/prevention systems
•□Routers and switches
•□Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)
•□Network Access Control (NAC)
•□Data Loss Prevention (DLP)
•□Unified Threat Management (UTM)
6.6 - Secure wireless communications
•□Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
•□Authentication and encryption protocols (e.g., Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (
6.7 Secure and monitor Internet of Things (IoT) (e.g., configuration, network isolation, firmware updates, End of Life (EOL)
7.1 - Identify and analyze malicious code and activity
•□Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless, ap
•□Malware countermeasures (e.g., scanners, anti-malware, containment and remediation, software security)
•□Types of malicious activity (e.g., insider threat, data theft, distributed denial of service (DDoS), botnet, zero-day ex
•□Malicious activity countermeasures (e.g., user awareness/training, system hardening, patching, isolation, data loss

- Social engineering methods (e.g., SPAM email, phishing/smishing/vishing, impersonation, scarcity, whaling)
- Behavior analytics (e.g., machine learning, Artificial Intelligence (AI), data analytics)

7.2 - Implement and operate endpoint device security

- Host-based intrusion prevention system (HIPS)
- Host-based intrusion detection system (HIDS)
- Host-based firewalls
- Application white listing
- Endpoint encryption (e.g., full disk encryption)
- Trusted Platform Module (TPM) (e.g., hardware security module management)
- Secure browsing (e.g., digital certificates)
- Endpoint detection and response (EDR)

7.3 - Administer and manage mobile devices

- Provisioning techniques (e.g., corporate owned, personally enabled (COPE), Bring Your Own Device (BYOD), Mobil
- Containerization
- Encryption
- Mobile application management

7.4 - Understand and configure cloud security

- Deployment models (e.g., public, private, hybrid, community)
- Service models (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS
- Virtualization (e.g., hypervisor, Virtual Private Cloud (VPC))
- Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery, shadow inform
- Data storage, processing, and transmission (e.g., archiving, backup, recovery, resilience)
- Third-party/Outsourcing requirements (e.g., service-level agreement (SLA), data portability/ privacy/destruction/a
- Shared responsibility model

7.5 - Operate and maintain secure virtual environments

- Hypervisor (i.e., Type 1 (e.g., bare metal), Type 2 (e.g., software))
- Virtual appliances
- Containers

- Continuity and resilience
- Storage management (e.g., data domain)
- Threats, attacks, and countermeasures (e.g., brute-force attack, virtual machine escape, threat hunting)

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to t

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

ISC2 recommends that SSCP candidates review exam policies and procedures prior to registering for the examination. Read the comp

A safe and secure cyber world

The Center for Cyber Safety & EducationISC2 CareersCommunityBlog

Frequently Asked QuestionsContact UsPolicies and Procedures

ISC2 Authorized China AgencyISC2 Japan

© Copyright 1996-2025. ISC2, Inc. All Rights Reserved.

All contents of this site constitute the property of ISC2, Inc. and may not be copied, reproduced or distributed without prior

Sitemap

SSCP Exam Outline

Agree to ISC2 policies

Top of Form

back to previous step

Bottom of Form

Top of Form

CC: Certified in Cybersecurity (CC)

Bottom of Form

Top of Form

ISC2 policies

Admission Policy

Plan to arrive at your test center at least **30 minutes** before your exam start time. To check in for your appointment the follo

· Show two (2) valid, unexpired forms of personal ID (examples include: government issued ids, passports, etc.). Both must ha

- **Unacceptable form of ID: Digital IDs** (A digital ID is an electronic representation of personally identifying ir

For additional information regarding the Aadhaar ID, please visit Aadhaar ID Policy for Pearson VUE.

- Minors under 18 – Minor must be accompanied by a parent or guardian on the day of exam.
  - Please refer for ID requirements for minors, https://www.isc2.org/exams/exam-day
- Provide your signature.
- Submit to a palm vein scan (unless expressly prohibited by law).
- Have your photo taken. Hats, scarves, and coats may not be worn for your photo. Additionally, you may not wear
- Leave your personal belongings outside the testing room. You will have access to secure storage. As storage space
- Receive a short orientation from the Test Administrator (TA). After the orientation, the TA will escort you to a test
- Sign and agree to the Non-Disclosure Agreement that will be presented at the beginning of your exam. Please take a momer

Where selected by your Test Sponsor, you agree that Pearson VUE will collect your palm vein pattern at the test center on the day of

Reschedule Policy

- If you wish to reschedule your exam appointment, you must contact Pearson VUE.
- There is no fee for rescheduling the Certified in Cybersecurity (CC) exam. For all other certifications, there is a US$
- If you choose to **go online to reschedule** your appointment, you must do so **at least 48 hours prior to your appoin**
- If you choose to **call the Pearson customer support team to reschedule**, you must do so **at least 24 hours prior to**
- If you do not reschedule your exam appointment without proper advanced notice, as outlined above, it will result
- Once scheduled you have up to 365 days to sit for your exam. Failure to sit for your examination within 365 days v

Cancellation Policy

- If you wish to cancel your exam appointment, you must contact Pearson VUE.
- There is no fee for canceling the Certified in Cybersecurity (CC) exam. For all other certifications, there is a US$10
- If you choose to **go online to cancel** your appointment, you must do so **at least 48 hours prior to your appointmer**
- If you choose to call the Pearson customer support team to cancel, you must do so at least 24 hours prior to your appointm
- If you do not cancel your exam appointment without proper advanced notice, as outlined above, it will result in a

Additional Information

ISC2 Terms and Conditions

- ISC2 requires that all candidates for certification read and accept the terms and conditions set forth here: https://www.isc2

Non-Disclosure Agreement (NDA)

- Failure to read or accept the ISC2 NDA agreement within the allotted five minutes will result in exam termination

Important Information on ISC2 Exams

- One of the benefits to candidates taking an examination via Computer-Based Testing is that most candidates rece
- ISC2 offers two types of computer-based exams – linear and adaptive – however neither exam type allows for can

· Frequently asked questions (FAQs) and answers for common inquiries that can be found here: https://www.isc2.org/Freque

Accommodations Policy

ISC2 provides reasonable and appropriate accommodations for people who have a documented need for exam accommodations. Acc

Top of Form

Cart

Bottom of Form

Collapsed, toggle side navigation to expand

Edit my profile Tshingombe Tshingombe Tshitadi

ISC2 ID: 1907033

· Dashboard

· My Profile

-

-

· Sign out

Top of Form

Bottom of Form

Almost there...

Top of Form

back to previous step

Bottom of Form

Top of Form

Confirm Order Details

Description	Details	Price
Exam	Appointment	199
CC: Certified in Cybersecurity (CC)	Friday, March 14, 2025	
Language: English	Start time: 8:00 AM Africa/Johannesburg - SAST	
Length: 120 minutes	Location	

Pearson Professional Centers- Johannesburg
Pearson VUE
6th Floor Sandton City Office Tower
Sandton City Shopping Centre
158 5th Street, SANDTON
Johannesburg
2146
South Africa
Payment Details
Exams for
Name:
Tshingombe Tshingombe Tshitadi

ISC2 ID:		
	1907033	
Order Total		
Subtotal:		199
Tax:		0
TOTAL DUE:	USD 199.00	
	USD 199.00	

Bottom of Form

Pearson VUE, so you can schedule your exam, contact information can be found at www.pearsonvue.com/isc2/contact.

Accommodations are not a guarantee of improved performance or exam completion. Once an initial exam appointment is s

Bottom of Form

Agree to ISC2 policies

Top of Form

back to previous step

Bottom of Form

Top of Form

CCSP: Certified Cloud Security Professional (CCSP)

CGRC: Certified in Governance Risk and Compliance

CISSP: Certified Information Systems Security Professional

CSSLP: Certified Secure Software Lifecycle Professional

ISSAP: Information Systems Security Architecture Professional

ISSMP: Information Systems Security Management Professional

SSCP: Systems Security Certified Practitioner

Certification Exam Outline

Effective Date: November 15, 2022

ISSMP Certification Exam Outline

About CISSP-ISSMP

The Information Systems Security Management Professional (ISSMP) is a CISSP who specializes in establishing, presenting and governing information security programs and demonstrates management and leadership skills. CISSP-ISSMPs direct the alignment of security programs with the organization's mission, goals and strategies in order to meet enterprise financial and operational requirements in support of its desired risk position.

The broad spectrum of topics included in the CISSP-ISSMP Common Body of Knowledge (CBK®) ensure its

relevancy across all disciplines in the field of information security management. Successful candidates are competent in the following six domains:

- Leadership and Business Management
- Systems Lifecycle Management
- Risk Management
- Threat Intelligence and Incident Management
- Contingency Management
- Law, Ethics and Security Compliance Management

Experience Requirements

Candidates must be a CISSP in good standing and have two years cumulative paid work experience in one or more of the six domains of the CISSP-ISSMP CBK. You can learn more about CISSP-ISSMP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP-Concentrations#steps-to-certification.

Accreditation

CISSP-ISSMP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CISSP-ISSMP. Conducted at

regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that

are performed by security professionals who are engaged in the profession defined by the CISSP-ISSMP. The

results of the JTA are used to update the examination. This process ensures that candidates are tested on the

topic areas relevant to the roles and responsibilities of today's practicing information security professionals.3

ISSMP Certification Exam Outline

CISSP-ISSMP Examination Information

CISSP-ISSMP Examination Weights

Length of exam
3 hours
Number of items
125
Item format
Multiple choice
Passing grade
Exam availability
Testing center

700 out of 1000 points
English
Pearson VUE Testing Center
Domains
Weight
1. Leadership and Business Management
20%
2. Systems Lifecycle Management
18%
3. Risk Management
19%
4. Threat Intelligence and Incident Management
17%
5. Contingency Management
15%
6. Law, Ethics and Security Compliance Management

11%

Total: 100%4

ISSMP Certification Exam Outline

Domain 1:

Leadership and Business Management

1.1 Establish security's role in organizational culture, vision and mission

» Define information security program vision and mission

» Align security with organizational goals, objectives and values

» Define security's relationship to the overall business processes

» Define the relationship between organizational culture and security

1.2 Align security program with organizational governance

» Identify and navigate organizational governance structure

» Validate roles of key stakeholders

» Validate sources and boundaries of authorization

» Advocate and obtain organizational support for security initiatives

1.3 Define and implement information security strategies

» Identify security requirements from business initiatives

» Evaluate capacity and capability to implement security strategies

» Manage implementation of security strategies

» Review and maintain security strategies

» Prescribe security architecture and engineering theories, concepts and methods

1.4 Define and maintain security policy framework Determine applicable external standards

» Determine applicable external standards

» Determine data classification and protection requirements

» Establish internal policies

» Advocate and obtain organizational support for policies

» Develop procedures, standards, guidelines and baselines

» Ensure periodic review of security policy framework

» Define roles and responsibilities

» Determine and manage team accountability

» Build cross-functional relationships

» Resolve conflicts between security and

other stakeholders
» Identify communication bottlenecks
and barriers
» Integrate security controls into human
resources processes
» Evaluate service management agreements
(e.g., risk, financial)
» Govern managed services
(e.g., infrastructure, cloud services)
» Manage impact of organizational change (e.g.,
mergers and acquisitions, outsourcing)
» Ensure that appropriate regulatory compliance
statements and requirements are included in
contractual agreements
» Monitor and enforce compliance with
contractual agreements
1.5 Manage security requirements in contracts and agreements

1.6 Manage security awareness and training programs

» Promote security programs to key stakeholders

» Identify needs and implement training programs by target segment

» Monitor and report on effectiveness of security awareness and training programs

1.7 Define, measure and report security metrics

» Identify Key Performance Indicators (KPI)

» Associate Key Performance Indicators (KPI) to the risk posture of the organization

» Use metrics to drive security program development and operations

1.8 Prepare, obtain and administer security budget

» Prepare and secure annual budget

» Adjust budget based on evolving risks and threat landscape

» Manage and report financial responsibilities

1.9 Manage security programs

1.10 Apply product development and project management principles

» Incorporate security into project lifecycle

» Identify and apply appropriate project management methodology

» Analyze project time, scope and cost relationship6

ISSMP Certification Exam Outline

2.1 Manage integration of security into Systems Development Life Cycle (SDLC)

» Integrate information security gates (decision points) and requirements into lifecycle

» Implement security controls into system lifecycle

» Oversee security configuration management (CM) processes

2.2 Integrate new business initiatives and emerging technologies into the

security architecture

» Integrate security into new business initiatives and emerging technologies

» Address impact of new business initiatives on security posture

2.3 Define and oversee comprehensive vulnerability management programs

(e.g., vulnerability scanning, penetration testing, threat analysis)

» Identify, classify and prioritize assets, systems and services based on criticality to business

» Prioritize threats and vulnerabilities

» Manage security testing

» Manage mitigation and/or remediation of vulnerabilities based on risk

2.4 Manage security aspects of change control

» Integrate security requirements with change control process

» Identify and coordinate with the stakeholders

» Manage documentation and tracking

» Ensure policy compliance (e.g., continuous monitoring)

Domain 2:

Systems Lifecycle Management 7

Domain 3:

Risk Management

3.1 Develop and manage a risk management program

» Identify risk management program objectives

» Communicate and agree on risk management objectives with risk owners and other stakeholders

» Determine scope of organizational risk program

» Identify organizational security risk tolerance/appetite

» Obtain and verify organizational asset inventory

» Analyze organizational risks

» Determine countermeasures, compensating and mitigating controls

» Perform cost-benefit analysis (CBA) of risk treatment options

3.2 Conduct risk assessments

» Identify risk factors

3.3 Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk)

» Identify supply chain security risk requirements

» Integrate supply chain security risks into organizational risk management

» Validate security risk control within the supply chain

» Monitor and review the supply chain security risks

ISSMP Certification Exam Outline

4.1 Establish and maintain threat intelligence program

» Aggregate threat data from multiple threat intelligence sources

» Conduct baseline analysis of network traffic, data and user behavior

» Detect and analyze anomalous behavior patterns for potential concerns

» Conduct threat modeling

» Identify and categorize an attack

» Correlate related security event and threat data

» Create actionable alerting to appropriate resources

4.2 Establish and maintain incident handling and investigation program

» Develop program documentation

» Establish incident response case management process

» Establish incident response team

» Apply incident management methodologies

» Establish and maintain incident handling process

» Establish and maintain investigation process

» Quantify and report financial and operational impact of incidents and investigations to stakeholders

» Conduct root cause analysis (RCA)

Domain 4:

Threat Intelligence and Incident

Management 9

5.1 Facilitate development of contingency plans

» Identify and analyze factors related to the Continuity of Operations Plan (COOP)

» Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification)

» Identify and analyze factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)

» Coordinate contingency management plans with key stakeholders

» Define internal and external crisis communications plans

» Define and communicate contingency roles and responsibilities

» Identify and analyze contingency impact on business processes and priorities

» Manage third-party contingency dependencies

» Prepare security management succession plan

5.2 Develop recovery strategies

» Identify and analyze alternatives

» Recommend and coordinate recovery strategies

» Assign recovery roles and responsibilities

5.3 Maintain contingency plan, Continuity of Operations Plan (COOP), business continuity plan (BCP) and disaster recovery plan (DRP)

» Plan testing, evaluation and modification

» Determine survivability and resiliency capabilities

» Manage plan update process

5.4 Manage disaster response and recovery process

» Declare disaster

» Implement plan

» Restore normal operations

» Gather lessons learned

» Update plan based on lessons learned

Domain 5:

Contingency Management 10

6.1 Identify the impact of laws and regulations that relate to information security

6.2 Adhere to the (ISC)

2

Code of Ethics as related to management issues

6.3 Validate compliance in accordance with applicable laws, regulations and industry

best practices

6.4 Coordinate with auditors and regulators in support of the internal and external

audit processes

6.5 Document and manage compliance exceptions

» Identify and document compensating controls and workarounds

» Report and obtain authorized approval of risk waiver

Domain 6:

Law, Ethics and Security Compliance

Management

» Identify applicable privacy laws

» Identify legal jurisdictions the organization and

users operate within (e.g., trans-border data flow)

» Identify export laws

» Identify intellectual property (IP) laws

» Identify applicable industry regulations

» Identify and advise on non-compliance risks

» Inform and advise senior management

» Evaluate and select compliance framework(s)

» Implement the compliance framework(s)

» Define and monitor compliance metrics

» Plan

» Schedule

» Coordinate audit activities

» Evaluate and validate findings

» Formulate response

» Validate implemented mitigation and

remediation actions11

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing

relevant resources that pertain to the CBK and identifying areas of study that may need

additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)2 recommends that CISSP-ISSMP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Exams/Before-Your-Exam.

Legal Info

For any questions related to (ISC)

’s legal policies, please contact the (ISC)2 Legal Department at legal@isc2.org.

Any Questions?

(ISC)2 Americas

Tel: +1.866.331.ISC2 (4722)

Email: info@isc2.org

(ISC)2 Asia-Pacific

Tel: +(852) 28506951

Email: isc2asia@isc2.org

(ISC)2 EMEA

Tel: +44 (0)203 300 1625

Email: info-emea@isc2.org

About CISSP-ISSEP

The Information Systems Security Engineering Professional (ISSEP) is a CISSP who specializes in the practical application of systems engineering principles and processes to develop secure systems. An ISSEP analyzes organizational needs, defines security requirements, designs security architectures, develops secure designs, implements system security, and supports system security assessment and authorization for government and industry.

The broad spectrum of topics included in the ISSEP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of security engineering. Successful candidates are competent in the following five domains:

• Systems Security Engineering Foundations

- Risk Management
- Security Planning and Design
- Systems Implementation, Verification and Validation
- Secure Operations, Change Management and Disposal

Experience Requirements

Candidates must be a CISSP in good standing and have two years cumulative paid work experience in one or more of the five domains of the CISSP-ISSEP CBK. You can learn more about CISSP-ISSEP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP-ISSEP/experience-requirements.

Accreditation

CISSP-ISSEP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the ISSEP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the ISSEP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

ISSEP Certification Exam Outline

CISSP-ISSEP Examination Information

CISSP-ISSEP Examination Weights

Length of exam
3 hours
Number of items
125
Item format
Multiple choice
Passing grade
700 out of 1000 points
Exam availability
English
Testing center
Pearson VUE Testing Center

Domains

Weight
1. Systems Security Engineering Foundations
25%
2. Risk Management
14%
3. Security Planning and Design
30%
4. Systems Implementation, Verification and Validation
14%
5. Secure Operations, Change Management
and Disposal
17%
Total: 100%4
ISSEP Certification Exam Outline
Domain 1:
Systems Security Engineering Foundations
1.1 Apply systems security engineering fundamentals

1.2 Execute systems security engineering processes

1.3 Integrate with applicable system development methodology

1.4 Perform technical management

1.5 Participate in the acquisition process

1.6 Design Trusted Systems and Networks (TSN)

» Understand systems security engineering trust concepts and hierarchies

» Identify the relationships between systems and security engineering processes

» Apply structural security design principles

» Integrate security tasks and activities

» Verify security requirements throughout the process

» Integrate software assurance methods

» Perform project planning processes

» Perform project assessment and control

processes
» Perform decision management processes
» Perform risk management processes
» Perform configuration management processes
» Perform information management processes
» Perform measurement processes
» Perform Quality Assurance (QA) processes
» Identify opportunities for security process
automation
» Identify organizational security authority
» Identify system security policy elements
» Integrate design concepts
(e.g., open, proprietary, modular)
» Prepare security requirements for acquisitions
» Participate in selection process
» Participate in Supply Chain Risk Management
(SCRM)

» Participate in the development and review of

contractual documentation5

ISSEP Certification Exam Outline

Domain 2:

Risk Management

2.1 Apply security risk management principles

2.2 Address risk to system

2.3 Manage risk to operations

» Establish risk context

» Identify system security risks

» Perform risk analysis

» Perform risk evaluation

» Recommend risk treatment options

» Document risk findings and decisions

» Determine stakeholder risk tolerance

» Identify remediation needs and other system changes

» Determine risk treatment options

» Assess proposed risk treatment options

» Recommend risk treatment options

» Align security risk management with Enterprise Risk Management (ERM)

» Integrate risk management throughout the lifecycle

ISSEP Certification Exam Outline

3.1 Analyze organizational and operational environment

3.2 Apply system security principles

3.3 Develop system requirements

3.4 Create system security architecture and design

Domain 3:

Security Planning and Design

» Capture stakeholder requirements

» Identify relevant constraints and assumptions

» Assess and document threats

» Determine system protection needs

» Develop Security Test Plans (STP)

» Incorporate resiliency methods to address threats

» Apply defense-in-depth concepts

» Identify fail-safe defaults

» Reduce Single Points of Failure (SPOF)

» Incorporate least privilege concept

» Understand economy of mechanism

» Understand Separation of Duties (SoD) concept

» Develop system security context

» Identify functions within the system and security

Concept of Operations (CONOPS)

» Document system security requirements baseline

» Analyze system security requirements

» Develop functional analysis and allocation

» Maintain traceability between specified design

and system requirements

» Develop system security design components

» Perform trade-off studies

» Assess protection effectiveness

Domain 4:

Systems Implementation, Verification and Validation

4.1 Implement, integrate and deploy security solutions

4.2 Verify and validate security solutions

» Perform system security implementation and integration

» Perform system security deployment activities

» Perform system security verification

» Perform security validation to demonstrate security controls meet stakeholder security requirements

Domain 5:

Secure Operations, Change Management and Disposal

5.1 Develop secure operations strategy

5.2 Participate in secure operations

5.3 Participate in change management

5.4 Participate in the disposal process

» Specify requirements for personnel conducting operations

» Contribute to the continuous communication with stakeholders for security relevant aspects of the system

» Develop continuous monitoring solutions and processes

» Support the Incident Response (IR) process

» Develop secure maintenance strategy

» Participate in change reviews

» Determine change impact

» Perform verification and validation of changes

» Update risk assessment documentation

» Identify disposal security requirements

» Develop secure disposal strategy

» Develop decommissioning and disposal procedures

» Audit results of the decommissioning and disposal process

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that ISSEP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)2 Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Americas

Tel: +1-866-331-ISC2(4722)

Email: membersupport@isc2.org

(ISC)² Asia Pacific

Tel: +852-2850-6951

Email: membersupportapac@isc2.org

(ISC)² EMEA

Tel: +44-203-960-7800

Email: membersupportemea@isc2.org

Attachments

Rate this

Details

Lenovo and Intel are Driving AI Innovation at the Edge

Flynn Maloy, Chief Marketing Officer of Lenovo ISG

Jan 23 2025| 0 mins

Lenovo and Intel's long-standing partnership is transforming industries by bringing cutting-edge AI solutions to the edge and

State of Cloud 2025: Navigating EMEA's Cloud Revolution

John Bradshaw, Director of Cloud Computing Technology and Strategy, EMEA, Akamai & Bryan Glick, Editor in Chief, Comput

Feb 27 2025| 18 mins

Boris Cipot, Senior Security Engineer

Sep 05 2024| 30 mins

Python is a fast, platform-agnostic, and easy-to-learn programming language that is suited for beginners and experienced

Nate Avery, Outbound Product Manager - Google | Jackie Porter, Director of Product - Gitlab | Torsten Volk, Principal Analy

Dec 04 2024| 28 mins

Seamless Edge Deployment and Management with Lenovo and Intel

Blake Kerrigan, Senior Director, ThinkEdge Business Group

Jan 23 2025| 1 mins

Sort by

Career Opportunity

Senior Applied Scientist – Copilot Team

Posted: March 3, 2025

Location: Beijing, China

Research Area(s): Artificial intelligence

We are inviting you to join the Copilot Team, where we are redefining the future of AI-powered experiences. The Copilot Te

Career Opportunity

Senior Applied AI Engineer – Microsoft Security AI Research team

Posted: March 3, 2025

Location: Remote (within US)

Research Area(s): Artificial intelligence, Security, privacy, and cryptography

Join the vanguard of cybersecurity innovation with the Microsoft Security AI Research team. We are on the lookout for an A

Career Opportunity

Data Scientist II – Microsoft Security

Posted: March 1, 2025

Location: Remote (within US); United States

Research Area(s): Artificial intelligence, Data platforms and analytics, Human-computer interaction, Security, privacy, and cr

The AI Personalization, Feedback, and Analytics team ensures that Security Copilot, Microsoft's GenAI platform, delivers ada

Career Opportunity

Senior Applied Scientist – Power Apps

Posted: March 1, 2025

Location: Redmond, WA, US; Remote (within US)

Research Area(s): Algorithms, Artificial intelligence, Data platforms and analytics

The Power Apps team at Microsoft is looking to hire a Senior Applied Scientist. As a team, we are very customer focused and

Career Opportunity

Applied Scientist II – Power Apps

Posted: March 1, 2025

Location: Redmond, WA, US; Remote (within US)

Research Area(s): Algorithms, Artificial intelligence, Data platforms and analytics, Programming languages and software engi

The Power Apps team at Microsoft is looking to hire an Applied Scientist II. As a team, we are very customer focused and dri

Career Opportunity

Principal Applied Scientist – Advanced Autonomy and Applied Robotics

Posted: March 1, 2025

Location: Redmond, WA, US

Research Area(s): Artificial intelligence, Hardware and devices, Human-computer interaction, Technology for emerging mark

Within Microsoft's Strategic Missions and Technologies (SMT) division, the Advanced Autonomy and Applied Robotics team

Career Opportunity

Senior Applied Scientist – Advanced Autonomy and Applied Robotics

Posted: March 1, 2025

Location: Redmond, WA, US

Research Area(s): Artificial intelligence, Hardware and devices, Human-computer interaction, Technology for emerging mark

Within Microsoft's Strategic Missions and Technologies (SMT) division, the Advanced Autonomy and Applied Robotics team

Career Opportunity

Principal Researcher – Generative AI – Microsoft Research AI Frontiers

Posted: March 1, 2025

Location: New York, NY, US; Redmond, WA, US

Research Area(s): Artificial intelligence

We are seeking a Principal Researcher to join our team and lead efforts on the advancement of Generative AI and Large Lan

Career Opportunity

Senior Applied Scientist

Posted: March 1, 2025

Location: Cairo, Egypt

Research Area(s): Artificial intelligence

In shaping the future of monetization for personalized AI assistants and pioneering innovation in the advertiser agentic spac

Career Opportunity

Principal Data Scientist – Real-Time Intelligence team

Posted: February 28, 2025

Location: Redmond, WA, US

Research Area(s): Artificial intelligence, Data platforms and analytics, Systems and networking

Microsoft Fabric's Real-Time Intelligence team is leading the transformation of real-time analytics in the world of data.We are hiring a Princip

engineering

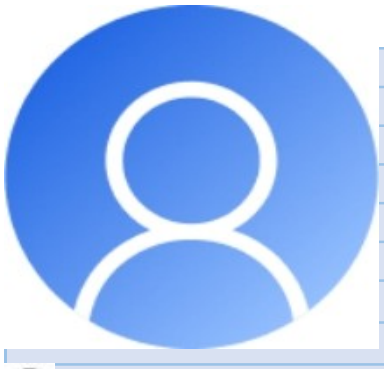
Inbox

tshingombe fiston <tshingombefiston@gmail.com>

Mon, Mar 3, 3:19 PM (18 hours ago)

to me

namics 365 Community / My Profile



CU03031227-0

Stats

0 Comments

0 Posts

1 Likes

0 Questions

My activity

Achievements

.

Personal information

.

Achievements

.

Notifications

.

Notification settings

.

Quick responses

Personal information

Email

tshingombefiston@gmail.com

Confirmation

Registration details

Name

tshingombe tshitadi

Status

Registered

Registration ID

102231646

Quick Links

· Go to the Microsoft Research Forum Website

· Registration support

· Cancel registration

Please note: event emails will be sent to the email address you provided during registration. If you are not receiving event c

Microsoft is committed to your privacy. If you have questions surrounding how your registration is affected by the General Data Prote

Share the news you've registered!

Compare Microsoft 365 with Office

Best value for 2 to 6 people

Microsoft 365 Family

Subscription

R1 999,00/year

Buy now

Or buy at R199,00/month

Try free for 1 month

Microsoft 365 Personal

Subscription

R1 599,00/year

Buy now

Or buy at R159,00/month

Office Home 2024

One-time purchase for PC or Mac

R2 299,00

Buy now

	Microsoft 365 Family	Microsoft 365 Personal	Office Home 2024
Number of users	1 to 6 people	1 person	One PC or Mac
Number of accounts	1 to 6	1	One PC or Mac

Cloud storage	Up to 6 TB (1 TB per person)	1 TB	
Multiple devices and platforms	Included	Included	
Word, Excel, PowerPoint	Included	Included	Included
OneNote	Included	Included	Included
Outlook	Included	Included	
Ongoing technical support	Included	Included	
Microsoft Defender	Included	Included	
Microsoft Editor	Included	Included	
Clipchamp	Included	Included	
Microsoft Teams	Included	Included	
Access (PC only)	Included	Included	
Microsoft Forms	Included	Included	

· Learn more · Learn more · Learn more

Office Home & Business 2024

- One-time purchase for one PC or Mac
- Classic 2024 desktop versions of Word, Excel, PowerPoint, Outlook and OneNote
- Access to support resources

Buy now Learn more

to me

Feedback on Security Service Provider Application and Complaint Process

Application for Exemption Terms of Section 23(6)

Key Points:

- Applicant Information:
  - Full Name: Tshingombe Fiston
  - Date: January 18, 2025, 6:36 PM
  - Contact: Not provided
- Application Details:
  - Terms of Section 23(6) of the Private Security Industry Regulation Act 56 of 2001.

- Despite Section 23(1) and (2), the authority may register any applicant as a security service provider on
- Requirements include applicant's age, training, and clearance of any criminal offenses in the last ten yea

Particulars of Appellant:

- Full Name: Tshingombe Fiston
- Contact Address: Not provided
- Refusal Reasons:
  - Refusal to grant application for registration.
  - Refusal to renew registration.
  - Cancellation or suspension of registration.
  - Conviction of improper conduct.

Complaints Management Process:

- Statutory Mandate: Derived from the Private Security Regulation Act 56 of 2001.
- Complaint Definition: Dissatisfaction reported to PSIRA regarding the quality of service rendered by a private sec
- Complaint Handling: Complaints are processed, referred, or dealt with by PSIRA in accordance with the code of c

Security Equipment Definition:

- Types of Equipment:
  - Alarm systems, safes, satellite tracking devices.
  - Intrusion detection, access control, bomb detection, and fire detection devices.
  - Security containers, X-ray, and communication devices.

Improper Conduct:

- Examples:
  - Operating without registration.
  - Deploying unregistered security officers.
  - Failure to meet training and uniform standards.
  - Non-payment of prescribed wages and allowances.

Complaint Resolution:

- Time Frame: Standard period to finalize any complaint is 30 to 90 days.
- Common Complaints: Include wage disputes, improper conduct, and training deficiencies.

Digital Records:

- Last Updated: 12-05-2022
- Batch Numbers:
  - Batch 383731: Pending since June 28, 2024.

- Batch 383732: Termination pending since June 29, 2024.

Job Career Information:

- Current Status: Application for registration as a security officer in progress.
- Job Requirements:
  - Basic salary, education qualifications, and employment history.
  - Ability to work under pressure and interpret legislation.
  - High administrative skills and problem-solving abilities.

Investigation and Complaints:

- Details of Complaints:
  - Complainant Name: Tshingombe Fiston
  - Incident Date: July 14, 2023
  - Nature of Complaint: Dismissal from job, irregularities in exam processes, and issues with certification.

Legal and Administrative Actions:

- Court Cases:
  - Labour court cases and appeals.
  - Complaints lodged with various authorities including the Office of the Chief Justice.
- Outcomes:
  - Pending decisions and unresolved issues.
  - Requests for reviews and rescission rulings.

Training and Development:

- Police Community Support Officer (PCSO) Training:
  - Duration: One month initial training.
  - Key Areas: Radio procedures, evidence gathering, crime scene management, human rights, and diversity

Student Placement Programs:

- Areas of Placement:
  - Financial crime investigation.
  - Estate and asset management.
  - Construction and building engineering.
- Essential Skills:
  - Planning, organization, communication, technical skills, and teamwork.

Expression of Interest and Withdrawals:

- Record of Interest: Successfully withdrawn from certain roles.

- Feedback: Encouraged to explore other opportunities within the organization.

Freedom of Information Requests:

- Recent Requests:
  - Request for validation and information under the Freedom of Information Act.
  - Requirements for resubmission and personal data verification.

Integrity and Defense:

- Research Focus:
  - Issues related to justice, education, and low development.
  - Emphasis on technological support and criminal investigations.

Summary:

- Feedback: Comprehensive review of the application, complaint process, and training details provided. Emphasis

fiston inspected Independent of Police Conduct's Cyber Essentials certificate on Thursday 6th March 2025 - 08:06:54(GMT

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value

Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	Independent of Police Conduct		Independent of Police Conduct
Issued by	The IASME Consortium Ltd		The IASME Consortium Ltd
Certificate ID	29be4854-f18d-45f4-b5b4-cf3c9613c4b5		29be4854-f18d-45f4-b5b4-cf3c9613c4b5
Issued on	2022-12-09T13:18:38.476101+00:00		2022-12-09T13:18:38.476101+00:00
Date of certification	2022-12-09T13:18:00+00:00		2022-12-09T13:18:00+00:00
Valid to	2023-12-09T13:18:00+00:00		2023-12-09T13:18:00+00:00
Status	Expired		Expired
Extra data			
scope	Whole Organisation		Whole Organisation

About Us | User Agreement | Pricing | What's new? | Coming soon | Report issue or request feature

Copyright © 2019-2025 BlockMark Technologies Ltd. "blockmark", the BlockMark logo and the BM-in-a-square logo are regis

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:06:17(GMT)

tshingombe tshitadi fiston inspected NOW TEACH's Cyber Essentials certificate on Thursday 6th March 2025 - 08:06:17(GI

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	NOW TEACH	NOW TEACH	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	
Certificate ID	fe96bbd5-0cc4-4c18-b796-4f75b5e5d44f	fe96bbd5-0cc4-4c18-b796-	
Issued on	2024-07-30T14:49:32.065737+00:00	2024-07-30T14:49:32.065737+00:00	
Date of certification	2024-07-30T14:49:00+00:00	2024-07-30T14:49:00	
Valid to	2025-07-30T14:49:00+00:00	2025-07-30T14:49:00+00:00	
Status	Active	Active	

Extra data		
scope	Whole Organisation	Whole Organisation

PDF at time of inspection

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:05:08(GMT)

tshingombe tshitadi fiston inspected BLUE LIGHT PUBLISHING LIMITED Trading as POLICE PASS's Cyber Essentials certificat

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	BLUE LIGHT PUBLISHING LIMITED Trading as POLICE PASS	BLUE LIGHT PUBLISHIN	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	
Certificate ID	0ebe3fad-f94b-4f2e-a85f-962d536acca5	0ebe3fad-f94b-4f2e-a85f-962d536ac	

Issued on	2024-05-29T16:23:41.690928+00:00	2024-05-29T16:23:41.690928+00:00
Date of certification	2024-05-29T17:23:00+00:00	2024-05-29T17:23:00+00:00
Valid to	2025-05-29T17:23:00+00:00	2025-05-29T17:23:00+00:00
Status	Active	Active
Extra data		
scope	Whole Organisation	Whole Organisation

PDF at time of inspection

\

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:49:36(GMT)

tshingombe tshitadi fiston inspected SAFETY SHIELD GLOBAL LIMITED's Cyber Essentials certificate on Thursday 6th March

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value

Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	SAFETY SHIELD GLOBAL LIMITED		SAFETY SHIELD GLOBAL
Issued by	The IASME Consortium Ltd		The IASME Consortium Ltd
Certificate ID	3e312a03-d76f-4194-b49d-6ebcef43434c		3e312a03-d76f-4194-b49d-6ebcef43434c
Issued on	2023-11-01T09:42:20.887845+00:00		2023-11-01T09:42:20.887845+00:00
Date of certification	2023-11-01T09:42:00+00:00		2023-11-01T09:42:00+00:00
Valid to	2024-11-01T09:42:00+00:00		2024-11-01T09:42:00+00:00
Status	Expired		Expired
Extra data			
scope	Whole Organisation		Whole Organisation

PDF at time of inspection

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:49:01(GMT)

tshingombe tshitadi fiston inspected Spillard Safety Systems Limited's Cyber Essentials Plus certificate on Thursday 6th Ma

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials Plus	Cyber Essentials Plus	
Issued to	Spillard Safety Systems Limited	Spillard Safety Systems	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	
Certificate ID	98240e15-5f1b-4dd2-8ea0-da63276762b4	98240e15-5f1b-4dd2-8ea0-da63276762	
Issued on	2024-01-03T11:54:43.575715+00:00	2024-01-03T11:54:43.575715+00:00	
Date of certification	2024-01-03T11:54:00+00:00	2024-01-03T11:54:00+00:00	
Valid to	2025-01-03T11:54:00+00:00	2025-01-03T11:54:00+00:00	
Status	Expired	Expired	
Extra data			

scope	Whole Organisation	Whole Organisation

PDF at time of inspection

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:47:55(GMT)

tshingombe tshitadi fiston inspected Business Safety Systems Limited's Cyber Essentials Plus certificate on Thursday 6th M

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials Plus	Cyber Essentials Plus	
Issued to	Business Safety Systems Limited	Business Safety Systems	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	
Certificate ID	16b1cc59-a0e5-4ab4-977b-e22e556140e2	16b1cc59-a0e5-4ab4-977b-	
Issued on	2024-08-16T11:11:35.401347+00:00	2024-08-16T11:11:35.401347+00:00	

Date of certification	2024-08-16T11:11:00+00:00	2024-08-16T11:11:00:00:00
Valid to	2025-08-16T11:11:00+00:00	2025-08-16T11:11:00+00:00
Status	Active	Active
Extra data		
scope	Whole Organisation	Whole Organisation

PDF at time of inspection

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:46:52(GMT)

tshingombe tshitadi fiston inspected LIGHTNING FIRE SAFETY SYSTEMS LTD's Cyber Essentials certificate on Thursday 6th

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	LIGHTNING FIRE SAFETY SYSTEMS LTD	LIGHTNING FIRE SAFETY	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	

Certificate ID	ca683bd6-86ec-4e29-9fbd-3f3d1398097b	ca683bd6-86ec-4e29-9fbd-3f3d13980
Issued on	2024-11-28T07:52:49.189801+00:00	2024-11-28T07:52:49.189801+00:00
Date of certification	2024-11-28T07:52:00+00:00	2024-11-28T07:52:00:00
Valid to	2025-11-28T07:52:00+00:00	2025-11-28T07:52:00+00:00
Status	Active	Active
Extra data		

scope	In scope are the devices and staff at the Waterlooville Office, including any home networks Waterlooville staff may work from. The scope excludes the devices and staff at the Leicestershire Office.	In scope are the devices and staff at the Waterlooville Office, including any home networks Waterlooville staff may work from. The scope excludes the devices and staff at the Leicestershire Office.

PDF at time of inspection

A certificate inspection by tshingombe tshitadi fiston

This certificate was inspected on Thursday 6th March 2025 - 08:58:01(GMT)

tshingombe tshitadi fiston inspected Securitas Security Services (UK) Limited's Cyber Essentials certificate on Thursday 6th

Below shows a comparison of the state of the certificate compared to its current state.

Field Name	Value when inspected	Current Value	Same Value
Certification scheme	Cyber Essentials	Cyber Essentials	
Issued to	Securitas Security Services (UK) Limited	Securitas Security Services	
Issued by	The IASME Consortium Ltd	The IASME Consortium Ltd	
Certificate ID	ff88f740-06ad-4c0b-8a54-8de97b382a8a	ff88f740-06ad-4c0b-8a54-8de97b382	
Issued on	2024-06-25T21:44:26.046017+00:00	2024-06-25T21:44:26.046017+00:00	
Date of certification	2024-06-25T21:44:00+00:00	2024-06-25T21:44:00:00:00	
Valid to	2025-06-25T21:44:00+00:00	2025-06-25T21:44:00+00:00	

Status	Active	Active

Skip to content

BLOCKMARK REGISTRY

apps

DASHBOARD

SWITCH ACCOUNT

£

tshingombe tshitadi fiston

keyboard_arrow_down

info

Inspected Certificates

View and manage your certificate inspections

-
-

Showing 1 - 19 of 19 certificates

Scheme	Current status	Status when inspected		
Cyber Essentials Plus	Active	Active		
Cyber Essentials	Expired	Expired	The IASME Consortium Ltd	
Cyber Essentials	Active	Active	The IASME Consortium Ltd	Tier-3 Security Ltd (t/a Huntsman Security)
Cyber Essentials	Active	Active	The IASME Consortium Ltd	Securitas Security Services (UK) Limited

Cyber Essentials Plus	Active	Active	The IASME Consortium Ltd	Securitas Security Services (UK) Limited
Cyber Essentials	Active	Active	The IASME Consortium Ltd	DEFENSOR LIFE SAFETY SYSTEMS LIMITED
Cyber Essentials	Expired	Expired	The IASME Consortium Ltd	SAFETY SHIELD GLOBAL LIMITED (Safety Shield Systems Global Ltd)
	11/1/2023, 11:42 AM	11/1/2024, 11:42 AM	3/6/2025, 10:49 AM	3e312a03-d76f-4194-b49d-6ebcef43434c

Cyber Essentials Plus	Expired	Expired	The IASME Consortium Ltd	Spillard Safety Systems Limited
Cyber Essentials Plus	Active	Active	The IASME Consortium Ltd	Business Safety Systems Limited
Cyber Essentials Plus	Expired	Expired	The IASME Consortium Ltd	Acclaim Safety Systems Ltd
Cyber Essentials	Active	Active	The IASME Consortium Ltd	LIGHTNING FIRE SAFETY SYSTEMS LTD

Cyber Essentials Plus	Active	Active	The IASME Consortium Ltd	Intelligent Safety Ltd trading as Hawk Safety
Cyber Essentials	Expired	Expired	The IASME Consortium Ltd	Independent of Police Conduct
Cyber Essentials	Active	Active	The IASME Consortium Ltd	NOW TEACH
Cyber Essentials	Active	Active	The IASME Consortium Ltd	BLUE LIGHT PUBLISHING LIMITED Trading as POLICE PASS

Cyber Essentials	Active	Active	The IASME Consortium Ltd	Police Now
Cyber Essentials Plus	Active	Active	The IASME Consortium Ltd	Police Now
Cyber Essentials Plus	Active	Active	The IASME Consortium Ltd	Metropolitan Police Friendly Society Limited
Cyber Essentials Plus	Expired	Expired	The IASME Consortium Ltd	Police Scotland and Scottish Police Authority

Copyright © 2019-2025 BlockMark Technologies Ltd. "blockmark", the BlockMark logo and the BM-in-a-square logo are regis

Applications

Sorry. This opportunity is expired. It is now too late to complete your application.

Title	Status	Action
Volunteer Police Cadet Leader	Application Update	ReviewVolunteer Police Cadet Leader

Volunteer Police Cadet Leader	Application Update	ReviewVolunteer Police Cadet Leader	
Vehicle Replacement Programme Manager - Band D - Counter Terrorism Policing HQ	Application Update	ReviewVehicle Replacement Programme Manager - Band D - Counter Terrorism Policing HQ	
Twickenham DWP Recruitment Event	Registration Update	ReviewTwickenham DWP Recruitment Event	
TSU Planner (DC) - Technical Intelligence Exploitation and Development team	Application Update	ReviewTSU Planner (DC) - Technical Intelligence Exploitation and Development team	

Travel Services – Band C Service Delivery Manager	Application Update	ReviewTravel Services – Band C Service Delivery Manager	
Thamesmead Recruitment Event	Registration Update	ReviewThamesmead Recruitment Event	
Technology Lead - Data & Analysis - Counter Terrorism Policing HQ	Application Update	ReviewTechnology Lead - Data & Analysis - Counter Terrorism Policing HQ	
Technical Training Manager - Technology CSC - Counter Terrorism Policing HQ	Application Update	ReviewTechnical Training Manager - Technology CSC - Counter Terrorism Policing HQ	

Technical Training Manager - Technology CSC - Counter Terrorism Policing HQ	Application Update	ReviewTechnical Training Manager - Technology CSC - Counter Terrorism Policing HQ	
Technical Support Operative	Application Update	ReviewTechnical Support Operative	
Tactical Policy Advisor – Robbery and Knife Crime team-DC	Application Update	ReviewTactical Policy Advisor – Robbery and Knife Crime team-DC	
Supplier Assurance Manager	Application Update	ReviewSupplier Assurance Manager	
Supplier Assurance Lead	Application Update	ReviewSupplier Assurance Lead	

Substantive Detective Inspector - DPS Specialist investigations	Application Update	ReviewSubstantive Detective Inspector - DPS Specialist investigations	
Student Placement - Real Estate Development - Programme Support Officer 2025/2026	Application Update	ReviewStudent Placement - Real Estate Development - Programme Support Officer 2025/2026	

Student Placement - Project Support Assistant - Strategy, Performance, and Planning - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Project Support Assistant - Strategy, Performance, and Planning - 2025/2026 - Counter Terrorism Policing HQ	
Student Placement - Project Support Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Project Support Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Programme Support Officer – Real Estate Development, Property Services Department 2024/2025	Application Update	ReviewStudent Placement - Programme Support Officer – Real Estate Development, Property Services Department 2024/2025	
Student Placement - Portfolio Office Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	Application Update	Review Student Placement - Portfolio Office Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Performance Analyst - MO14 Performance	Application Update	ReviewStudent Placement - Performance Analyst - MO14 Performance	
Student Placement - Media and Communication Administrator 2025/2026	Application Update	ReviewStudent Placement - Media and Communication Administrator 2025/2026	
Student Placement - Junior Service Designer - Technology - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Junior Service Designer - Technology - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Junior Project Manager - Technology - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Junior Project Manager - Technology - 2025/2026 - Counter Terrorism Policing HQ	
Student Placement - Junior DevOps Engineer - Technology - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Junior DevOps Engineer - Technology - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Forensic Business Assistant 2025/2026	Application Update	ReviewStudent Placement - Forensic Business Assistant 2025/2026	
Student Placement - Estate and Asset Management Placement Student – Real Estate Management, Property Services Department 2024/2025	Application Update	ReviewStudent Placement - Estate and Asset Management Placement Student – Real Estate Management, Property Services Department 2024/2025	

Student Placement - Construction and Building Engineering Services - Real Estate Development , Property Services Department 2024/2025	Application Update	ReviewStudent Placement - Construction and Building Engineering Services - Real Estate Development , Property Services Department 2024/2025	
Student Placement - Construction and Building Engineering 2025/2026	Application Update	ReviewStudent Placement - Construction and Building Engineering 2025/2026	

Student Placement - Communications Assistant - 2025/2026 - Communications - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Communications Assistant - 2025/2026 - Communications - Counter Terrorism Policing HQ	
Student Placement - Business Change Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Business Change Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Borders Assistant - Borders Operations Centre - 2025/2026 Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Borders Assistant - Borders Operations Centre - 2025/2026 Counter Terrorism Policing HQ	
Student Placement - Assurance and Standards Team Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Assurance and Standards Team Assistant - Change - 2025/2026 - Counter Terrorism Policing HQ	

Student Placement - Associate End User Computing Engineer - Technology - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Associate End User Computing Engineer - Technology - 2025/2026 - Counter Terrorism Policing HQ	
Student Placement - Analysis & Research Assistant - Data & Analysis - 2025/2026- Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Analysis & Research Assistant - Data & Analysis - 2025/2026- Counter Terrorism Policing HQ	

Student Placement - Accredited Financial Investigator - 2025/2026	Application Update	ReviewStudent Placement - Accredited Financial Investigator - 2025/2026	
Student Placement - Project / Research Assistant - Data & Analysis - 2025/2026 - Counter Terrorism Policing HQ	Application Update	ReviewStudent Placement - Project / Research Assistant - Data & Analysis - 2025/2026 - Counter Terrorism Policing HQ	
Strategy and Local Communications Manager(FTC for 12month)	Application Update	ReviewStrategy and Local Communications Manager(FTC for 12month)	

Strategy and Local Communications Manager	Application Update	ReviewStrategy and Local Communications Manager	
Staff Officer to Director of Intelligence & Covert Policing	Application Update	ReviewStaff Officer to Director of Intelligence & Covert Policing	
Staff Officer to Director General - Detective Inspector - SLT - Counter Terrorism Policing HQ	Application Update	ReviewStaff Officer to Director General - Detective Inspector - SLT - Counter Terrorism Policing HQ	

Staff Officer to Director General - Band C - SLT - Counter Terrorism Policing HQ	Application Update	ReviewStaff Officer to Director General - Band C - SLT - Counter Terrorism Policing HQ	
SQL Server Database Administrator - Counter Terrorism Policing HQ	Application Update	ReviewSQL Server Database Administrator - Counter Terrorism Policing HQ	
SQL Server Database Administrator - Counter Terrorism Policing HQ	Application Update	ReviewSQL Server Database Administrator - Counter Terrorism Policing HQ	

Specialist Operations Recovery Manager	Application Update	ReviewSpecialist Operations Recovery Manager	
Specialist Operations Recovery Driver - Perivale Car Pound	Application Update	ReviewSpecialist Operations Recovery Driver - Perivale Car Pound	
Specialist Crime - North - Homicide Barking - HOLMES Typist	Application Update	ReviewSpecialist Crime - North - Homicide Barking - HOLMES Typist	
SIU - Developing Threats Team - Detective Sergeant	Application Update	ReviewSIU - Developing Threats Team - Detective Sergeant	
Shift Team – CJ Offender Management Services	Application Update	ReviewShift Team – CJ Offender Management Services	

Service Design and Transition Manager - Band C - Technology - Counter Terrorism Policing HQ	Application Update	ReviewService Design and Transition Manager - Band C - Technology - Counter Terrorism Policing HQ	
Server Engineer - Technology - CSC - Counter Terrorism Policing HQ	Application Update	ReviewServer Engineer - Technology - CSC - Counter Terrorism Policing HQ	
Senior Server Engineer - Counter Terrorism Policing HQ	Application Update	ReviewSenior Server Engineer - Counter Terrorism Policing HQ	
Senior Safety Advisor First Aid	Application Update	ReviewSenior Safety Advisor First Aid	

Senior Project Manager, Met Business & Operational Support Services	Application Update	ReviewSenior Project Manager, Met Business & Operational Support Services	
Senior Project Manager - Change - Counter Terrorism Policing HQ	Application Update	ReviewSenior Project Manager - Change - Counter Terrorism Policing HQ	
Senior Project Manager	Application Update	ReviewSenior Project Manager	
Senior Project Manager	Application Update	ReviewSenior Project Manager	
Senior MetLaw Officer	Application Update	ReviewSenior MetLaw Officer	
Senior Media Officer	Application Update	ReviewSenior Media Officer	

Senior Manager - Biometrics (Band B)	Application Update	ReviewSenior Manager - Biometrics (Band B)	
Senior HR Policy Lead	Application Update	ReviewSenior HR Policy Lead	
Senior HR Business Advisor	Application Update	ReviewSenior HR Business Advisor	
Senior Development Operations Engineer - Band M - Counter Terrorism Policing HQ	Application Update	ReviewSenior Development Operations Engineer - Band M - Counter Terrorism Policing HQ	
Senior Design Standards Manager	Application Update	ReviewSenior Design Standards Manager	
Senior Content, Channels and Engagement Officer	Application Update	ReviewSenior Content, Channels and Engagement Officer	

Senior Application Operations Engineer - Technology CSC - Counter Terrorism Policing HQ	Application Update	ReviewSenior Application Operations Engineer - Technology CSC - Counter Terrorism Policing HQ	
Senior Administrative Assistant	Application Update	ReviewSenior Administrative Assistant	
Security Assurance Manager	Application Update	ReviewSecurity Assurance Manager	
Secure: Programme Delivery Senior Manager	Application Update	ReviewSecure: Programme Delivery Senior Manager	
Safety Camera Prosecutions Team Manager	Application Update	ReviewSafety Camera Prosecutions Team Manager	

Safety Camera Prosecutions Manager	Application Update	ReviewSafety Camera Prosecutions Manager	
Safety Camera Processing Clerk	Application Update	ReviewSafety Camera Processing Clerk	
Safety Academy QUAD Officer	Application Update	ReviewSafety Academy QUAD Officer	
Royalty and Specialist Protection - RaSP 400 Inspector	Application Update	ReviewRoyalty and Specialist Protection - RaSP 400 Inspector	
Royalty and Specialist Protection - Finance Administrator	Application Update	ReviewRoyalty and Specialist Protection - Finance Administrator	

Royalty and Specialist Protection - Finance Administrator	Application Update	ReviewRoyalty and Specialist Protection - Finance Administrator	
Review Officer	Application Update	ReviewReview Officer	
Resourcing Assistant	Application Update	ReviewResourcing Assistant	
Resource Management Office Manager	Application Update	ReviewResource Management Office Manager	
Research Officer for Intelligence Development Team (East) - Band E Role	Application Update	ReviewResearch Officer for Intelligence Development Team (East) - Band E Role	

Referencing & Vetting Insight and Governance Team Member	Application Update	ReviewReferencing & Vetting Insight and Governance Team Member	
Referencing & Vetting Insight and Governance Team Member	Application Update	ReviewReferencing & Vetting Insight and Governance Team Member	
Real Time Resourcing Desk Constable	Application Update	ReviewReal Time Resourcing Desk Constable	
Real Time Resource Desk Sergeant	Application Update	ReviewReal Time Resource Desk Sergeant	

RaSP Armed Deployment Management Unit (ADMU) PC	Application Update	ReviewRaSP Armed Deployment Management Unit (ADMU) PC	
RAID Manager - Change - Counter Terrorism Policing HQ	Application Update	ReviewRAID Manager - Change - Counter Terrorism Policing HQ	
Quality System Auditor	Application Update	ReviewQuality System Auditor	
Quality Assurance Operative	Application Update	ReviewQuality Assurance Operative	
Quality Assurance Lead	Application Update	ReviewQuality Assurance Lead	
Quality Assurance Lead	Application Update	ReviewQuality Assurance Lead	

PSO - Threat Assessment & Intelligence Unit - Intelligence Officer – Researcher	Application Update	ReviewPSO - Threat Assessment & Intelligence Unit - Intelligence Officer – Researcher	
ProtectUK Head of Digital Delivery Unit - NaCTSO - Counter Terrorism Policing HQ.	Application Update	ReviewProtectUK Head of Digital Delivery Unit - NaCTSO - Counter Terrorism Policing HQ.	
ProtectUK Head of Digital Content & Editorial NaCTSO - Counter Terrorism Policing HQ	Application Update	ReviewProtectUK Head of Digital Content & Editorial - NaCTSO - Counter Terrorism Policing HQ	

Project Support Officer	Application Update	ReviewProject Support Officer	
Project Manager	Application Update	ReviewProject Manager	
Project Adder - PC	Application Update	ReviewProject Adder - PC	
Programme Support Officer	Application Update	ReviewProgramme Support Officer	
Programme Manager - Change - Counter Terrorism Policing HQ	Application Update	ReviewProgramme Manager - Change - Counter Terrorism Policing HQ	
Programme Management Office Administrator	Application Update	ReviewProgramme Management Office Administrator	

Professional Standards Unit (MO12/MO4/CRIB) Band D	Application Update	ReviewProfessional Standards Unit (MO12/MO4/CRIB) Band D	
Professional Standards - Misconduct Hearings Unit - Case Manager	Application Update	ReviewProfessional Standards - Misconduct Hearings Unit - Case Manager	
Pound Officer Perivale	Application Update	ReviewPound Officer Perivale	
Police Sergeant – Proactive Firearms Team	Application Update	ReviewPolice Sergeant – Proactive Firearms Team	
Police prosecutor	Application Update	ReviewPolice prosecutor	
Police prosecutor	Application Update	ReviewPolice prosecutor	

Police Liaison Gateway Team	Application Update	ReviewPolice Liaison Gateway Team	
Police Constable – Proactive Firearms Team Tasking & Co-ordination	Application Update	ReviewPolice Constable – Proactive Firearms Team Tasking & Co-ordination	
Police Constable DPS - Professional Standard Unit	Application Update	ReviewPolice Constable DPS - Professional Standard Unit	
POLICE CONSTABLE - CYBER CRIME PROACTIVE UNIT	Application Update	ReviewPOLICE CONSTABLE - CYBER CRIME PROACTIVE UNIT	

PMO Lead - Change - Counter Terrorism Policing HQ	Application Update	ReviewPMO Lead - Change - Counter Terrorism Policing HQ	
Performance and Assurance Team Member	Application Update	ReviewPerformance and Assurance Team Member	
People & Development Lead, Operational Support Services	Application Update	ReviewPeople & Development Lead, Operational Support Services	
PC Facial Recognition Technologies Team	Application Update	ReviewPC Facial Recognition Technologies Team	
PC - MO6 Public Order Crime Team	Application Update	ReviewPC - MO6 Public Order Crime Team	

PC - Covert Human Intelligence Source (CHIS) Handler	Application Update	ReviewPC - Covert Human Intelligence Source (CHIS) Handler	
PA to DCS Band E	Application Update	ReviewPA to DCS Band E	
Outreach Support	Talent Bank - Withdrawn	ReviewOutreach Support	
Operations Support Officer	Application Update	ReviewOperations Support Officer	
Operations Manager	Application Update	ReviewOperations Manager	
Operations Lead - Superintendent	Application Update	ReviewOperations Lead - Superintendent	
Operations Inspector	Application Update	ReviewOperations Inspector	

Op Ford - Force Elected Official Advisor (FEOA) - Constable PaDP	Application Update	ReviewOp Ford - Force Elected Official Advisor (FEOA) - Constable PaDP	
Online Insight Session	Registration Update	ReviewOnline Insight Session	
Online Insight Session	Registration Update	ReviewOnline Insight Session	
Office Manager - Band D - MIR - SO15	Application Update	ReviewOffice Manager - Band D - MIR - SO15	
NPPF Step Two May 2024 Legal Exam - (Previously OSPRE) – Inspectors	Application Update	ReviewNPPF Step Two May 2024 Legal Exam - (Previously OSPRE) – Inspectors	

NPPF Step Two March 2025 Legal Exam (Previously OSPRE) - Sergeant	Application Update	ReviewNPPF Step Two March 2025 Legal Exam (Previously OSPRE) - Sergeant	
NPoCC Planner - Band E	Application Withdrawn	ReviewNPoCC Planner - Band E	
New Scotland Yard Insight Session	Registration Update	ReviewNew Scotland Yard Insight Session	
NCPP - CTSFO National Training Manager - Inspector - Counter Terrorism Policing HQ	Application Update	ReviewNCPP - CTSFO National Training Manager - Inspector - Counter Terrorism Policing HQ	

National Surveillance Scheduling Team and Capability Support - Detective Inspector - Counter Terrorism Policing HQ	Application Update	ReviewNational Surveillance Scheduling Team and Capability Support - Detective Inspector - Counter Terrorism Policing HQ	
National Referral Mechanism Coordinator	Application Update	ReviewNational Referral Mechanism Coordinator	
National Police Chiefs' Council - National Serious & Organised Crime Portfolio (NSOC) Project Manager	Application Update	ReviewNational Police Chiefs' Council - National Serious & Organised Crime Portfolio (NSOC) Project Manager	

National Police Chiefs Council - Programme Manager	Application Update	ReviewNational Police Chiefs Council - Programme Manager	
National Police Chiefs Council - Programme Manager	Application Update	ReviewNational Police Chiefs Council - Programme Manager	
National Police Chiefs Council - Internal Communications Manager	Application Update	ReviewNational Police Chiefs Council - Internal Communications Manager	
National Investigators Examination (NIE) - 3rd June 2025	Application Update	ReviewNational Investigators Examination (NIE) - 3rd June 2025	

National Firearms Instructor (NFI)	Application Update	ReviewNational Firearms Instructor (NFI)	
National Counter Terrorism Security Office (NaCTSO) – Venues and Public Spaces Unit-Detective Inspector - Counter Terrorism Policing HQ	Application Update	ReviewNational Counter Terrorism Security Office (NaCTSO) – Venues and Public Spaces Unit-Detective Inspector - Counter Terrorism Policing HQ	
Motorcycle Technician	Application Update	ReviewMotorcycle Technician	
Motor Vehicle Technician	Application Update	ReviewMotor Vehicle Technician	
Motor Vehicle Technician	Application Update	ReviewMotor Vehicle Technician	

Motor Vehicle Technician	Application Update	ReviewMotor Vehicle Technician	
MO7 Taskforce TSG -Police Sergeant	Application Update	ReviewMO7 Taskforce TSG -Police Sergeant	
MO7 Taskforce Mounted Branch Inspector	Application Update	ReviewMO7 Taskforce Mounted Branch Inspector	
MO3 Technical Surveillance Unit-DC - AV Ops	Application Update	ReviewMO3 Technical Surveillance Unit-DC - AV Ops	
MO2 Met Intel - ANPR Auditor - Innovation Deployment & Compliance Team	Application Update	ReviewMO2 Met Intel - ANPR Auditor - Innovation Deployment & Compliance Team	

MO19 Specialist Firearms Command – Development, Delivery, Equipment & Finance Sergeant	Application Update	ReviewMO19 Specialist Firearms Command – Development, Delivery, Equipment & Finance Sergeant	
MO19 Specialist Firearms Command - Tactical Firearms Commander Inspector (UNARMED)	Application Update	ReviewMO19 Specialist Firearms Command - Tactical Firearms Commander Inspector (UNARMED)	

MO19 Specialist Firearms Command - Tactical Firearms Commander Detective Inspector (UNARMED)	Application Update	ReviewMO19 Specialist Firearms Command - Tactical Firearms Commander Detective Inspector (UNARMED)	
MMU Vehicle Technician	Application Update	ReviewMMU Vehicle Technician	
Misconduct Hearings Unit - Usher	Application Update	ReviewMisconduct Hearings Unit - Usher	
MetLaw Clerk	Application Update	ReviewMetLaw Clerk	
MetLaw and Allocations Clerk	Application Update	ReviewMetLaw and Allocations Clerk	
MetCC Workforce Management Lead	Application Update	ReviewMetCC Workforce Management Lead	

MetCC Welfare Support Team Supervisor	Application Update	ReviewMetCC Welfare Support Team Supervisor	
MetCC Welfare Support Team Member	Application Update	ReviewMetCC Welfare Support Team Member	
MetCC Centre Facilities Support Staff	Application Update	ReviewMetCC Centre Facilities Support Staff	
MetCC Centre Facilities Supervisor	Application Update	ReviewMetCC Centre Facilities Supervisor	
Met Intel PC ANPR Investigations	Application Update	ReviewMet Intel PC ANPR Investigations	
Met Intel DS ANPR Investigations	Application Update	ReviewMet Intel DS ANPR Investigations	

Met Intel 24/7 Intelligence Officer	Application Update	ReviewMet Intel 24/7 Intelligence Officer	
Met Intel 24/7 - Intelligence Supervisor	Application Update	ReviewMet Intel 24/7 - Intelligence Supervisor	
Met Intel 24/7 - Intelligence Manager - Duty Officer	Application Update	ReviewMet Intel 24/7 - Intelligence Manager - Duty Officer	
Met Business Services - Talent Acquisition Manager	Application Update	ReviewMet Business Services - Talent Acquisition Manager	
Met Business Services - Talent Acquisition Lead	Application Update	ReviewMet Business Services - Talent Acquisition Lead	
Media Officer	Application Update	ReviewMedia Officer	

MBS Reporting Senior Analyst	Application Update	ReviewMBS Reporting Senior Analyst	
LMS Administrator	Application Update	ReviewLMS Administrator	
Licensing and Accreditation Training Development Officer - VAP's (NaCTSO) - Counter Terrorism Policing HQ	Application Update	ReviewLicensing and Accreditation Training Development Officer - VAP's (NaCTSO) - Counter Terrorism Policing HQ	
Licensing Admin Support Officer	Application Update	ReviewLicensing Admin Support Officer	
Leadership Facilitator	Application Withdrawn	ReviewLeadership Facilitator	

Leadership Academy Trainer/Facilitator	Application Update	ReviewLeadership Academy Trainer/Facilitator	
Leadership Academy Administration/Team Support	Application Update	ReviewLeadership Academy Administration/Team Support	
Leadership Academy Administration/Team Supervisor	Application Update	ReviewLeadership Academy Administration/Team Supervisor	
Lead Software Developer - Counter Terrorism Policing HQ	Application Update	ReviewLead Software Developer - Counter Terrorism Policing HQ	

Lead Dev Ops Engineer (Cloud Platform) - Technology CSC - Police Staff - Counter Terrorism Policing HQ	Application Update	ReviewLead Dev Ops Engineer (Cloud Platform) - Technology CSC - Police Staff - Counter Terrorism Policing HQ	
Lead Data Analyst in the Strategic Insight Unit	Application Update	ReviewLead Data Analyst in the Strategic Insight Unit	
Junior Software Developer - Counter Terrorism Policing HQ	Application Update	ReviewJunior Software Developer - Counter Terrorism Policing HQ	
Junior Data Engineer	Application Update	ReviewJunior Data Engineer	

Interest in being promoted to a Sergeant? Register your interest here and we will notify you when the promotion process launches.	Talent Bank - Withdrawn	ReviewInterest in being promoted to a Sergeant? Register your interest here and we will notify you when the promotion process launches.	
Interest in being promoted to a Chief Superintendent? Register your interest here and we will notify you when the promotion process launches.	Talent Bank - Withdrawn	ReviewInterest in being promoted to a Chief Superintendent? Register your interest here and we will notify you when the promotion process launches.	

Intelligence Officer - Public Order Public Safety Intelligence - MO2	Application Update	ReviewIntelligence Officer - Public Order Public Safety Intelligence - MO2	
Intelligence Officer - PC - Intelligence - Counter Terrorism Policing HQ	Application Update	ReviewIntelligence Officer - PC - Intelligence - Counter Terrorism Policing HQ	
Intelligence Officer - DC - Intelligence - Counter Terrorism Policing HQ	Application Update	ReviewIntelligence Officer - DC - Intelligence - Counter Terrorism Policing HQ	

Intelligence Officer - Bomb Data Centre - FMT - SO15	Application Update	ReviewIntelligence Officer - Bomb Data Centre - FMT - SO15	
Intelligence Manager – Public Order & Public Safety Intelligence - Inspector – MO2	Application Update	ReviewIntelligence Manager – Public Order & Public Safety Intelligence - Inspector – MO2	
Intelligence Manager - Public Order & Public Safety Intelligence - Detective Inspector - MO2	Application Update	ReviewIntelligence Manager - Public Order & Public Safety Intelligence - Detective Inspector - MO2	

Inspector to Chief Inspector Promotion Process 2024	Application Update	ReviewInspector to Chief Inspector Promotion Process 2024	
Inspector - NPoCC SIB	Application Update	ReviewInspector - NPoCC SIB	
Insight, Data and Evaluation Senior Manager	Application Update	ReviewInsight, Data and Evaluation Senior Manager	
Infrastructure Engineer	Application Update	ReviewInfrastructure Engineer	
IDD - Junior Business Design Analyst	Application Update	ReviewIDD - Junior Business Design Analyst	

Hub Coordination Team Manager - Band D - Prisons - Counter Terrorism Policing HQ	Application Update	ReviewHub Coordination Team Manager - Band D - Prisons - Counter Terrorism Policing HQ	
HR Performance and Reporting Manager	Application Update	ReviewHR Performance and Reporting Manager	
HR Performance and Reporting Lead	Application Update	ReviewHR Performance and Reporting Lead	
HR People Performance Improvement Team – Senior Lead	Application Update	ReviewHR People Performance Improvement Team – Senior Lead	

HR People Performance Improvement Team – Senior Lead	Application Update	ReviewHR People Performance Improvement Team – Senior Lead	
HR Change Support Officer	Application Update	ReviewHR Change Support Officer	
HR Administrator - Counter Terrorism Policing HQ	Application Update	ReviewHR Administrator - Counter Terrorism Policing HQ	
HOLMES Typist	Application Update	ReviewHOLMES Typist	
Higher Performance Analyst - Strategy, Planning & Performance - Counter Terrorism Policing HQ	Application Update	ReviewHigher Performance Analyst - Strategy, Planning & Performance - Counter Terrorism Policing HQ	

Higher Computer Aided Surveyor / 3D Specialist	Application Update	ReviewHigher Computer Aided Surveyor / 3D Specialist	
Health & Safety/Estates Manager - Band D - Counter Terrorism Policing HQ	Application Update	ReviewHealth & Safety/Estates Manager - Band D - Counter Terrorism Policing HQ	
Head of Visits and Events	Application Update	ReviewHead of Visits and Events	
Head of Visits and Events	Application Update	ReviewHead of Visits and Events	
Head of Security Architecture	Application Update	ReviewHead of Security Architecture	

Head of Portfolio Office (Met Business & Operational Support Services)	Application Update	ReviewHead of Portfolio Office (Met Business & Operational Support Services)	
Head of Portfolio Office (Met Business & Operational Support Services)	Application Update	ReviewHead of Portfolio Office (Met Business & Operational Support Services)	
Head of Data Literacy and Culture	Application Update	ReviewHead of Data Literacy and Culture	
Head of Data Engineering	Application Update	ReviewHead of Data Engineering	
Grievance Assessor	Application Update	ReviewGrievance Assessor	

Forensic Scientist	Application Update	ReviewForensic Scientist	
Forensic Management Team - Ops Support - Detective Sergeant - Counter Terrorism Policing SO15	Application Update	ReviewForensic Management Team - Ops Support - Detective Sergeant - Counter Terrorism Policing SO15	
Forensic Examiner – Forensic Firearms Unit (FFU)	Application Update	ReviewForensic Examiner – Forensic Firearms Unit (FFU)	
Forensic Collision Investigator – Trainee	Application Update	ReviewForensic Collision Investigator – Trainee	
Fleet Contract Lifecycle Support	Application Withdrawn	ReviewFleet Contract Lifecycle Support	

Fleet Administrator	Application Update	ReviewFleetAdministrator	
Fingerprint Team Leader	Application Update	ReviewFingerprintTeamLeader	
Financial Investigator	Application Update	ReviewFinancialInvestigator	
Finance Business Partner - Band M	Application Update	ReviewFinanceBusinessPartner-BandM	
Facial Identification Intelligence Researcher	Application Update	ReviewFacialIdentificationIntelligenceResearcher	
Facial Identification Intelligence Research Supervisor	Application Update	ReviewFacialIdentificationIntelligenceResearchSupervisor	

Experienced Intelligence Analyst	Application Update	ReviewExperienced Intelligence Analyst	
Equip for Service (EFS) Coordinator	Application Update	ReviewEquip for Service (EFS) Coordinator	
Equality Impact Assessment Manager	Application Update	ReviewEquality Impact Assessment Manager	
Enquiry Officer	Application Update	ReviewEnquiry Officer	
Electronics Senior Technologist	Application Update	ReviewElectronics Senior Technologist	
Electronics Development Manager	Application Update	ReviewElectronics Development Manager	
Electronics Development Manager	Application Update	ReviewElectronics Development Manager	

Electronics Development Engineer	Application Update	ReviewElectronics Development Engineer	
Electronics Development Engineer	Application Update	ReviewElectronics Development Engineer	
Electronics Development Engineer	Application Update	ReviewElectronics Development Engineer	
Electronics Development Engineer	Application Update	ReviewElectronics Development Engineer	
Edmonton Insight Session	Registration Update	ReviewEdmonton Insight Session	
DS - Public Order Crime Team	Application Update	ReviewDS - Public Order Crime Team	

Driver Assistance Centre Team Leader	Application Update	ReviewDriver Assistance Centre Team Leader	
DPS Intelligence Bureau - Integrity Screening Unit -Detective Constable (Substantive)	Application Update	ReviewDPS Intelligence Bureau - Integrity Screening Unit - Detective Constable (Substantive)	
DPS Digital Exploitation Team: Digital Intelligence Analyst - Anti-Corruption and Abuse Command	Application Update	ReviewDPS Digital Exploitation Team: Digital Intelligence Analyst - Anti-Corruption and Abuse Command	

DNA Services Consultant - BIOMETRICS UNIT (Band L)	Application Update	ReviewDNA Services Consultant - BIOMETRICS UNIT (Band L)	
Distribution Driver	Application Update	ReviewDistribution Driver	
Disruptions & APMIS Lead	Application Update	ReviewDisruptions & APMIS Lead	
Disclosure Support (deputy to Disclosure Manager, Economic Crime)	Application Update	ReviewDisclosure Support (deputy to Disclosure Manager, Economic Crime)	
Digital Strategy Advisor - Digital Forensics	Application Update	ReviewDigital Strategy Advisor - Digital Forensics	
Digital Strategy Advisor - Digital Forensics	Application Update	ReviewDigital Strategy Advisor - Digital Forensics	

Digital Project Officer - NDES Service 3 - SO15	Application Update	ReviewDigital Project Officer - NDES Service 3 - SO15	
Digital Operations - Digital Investigator (DMI) - PC	Application Update	ReviewDigital Operations - Digital Investigator (DMI) - PC	
Digital Forensic Technician	Application Update	ReviewDigital Forensic Technician	
Digital Forensic Manager	Application Update	ReviewDigital Forensic Manager	
Digital Engagement Officer	Application Update	ReviewDigital Engagement Officer	
Development Technician - Software Developer	Application Update	ReviewDevelopment Technician - Software Developer	
Development Technician - Software Developer	Application Update	ReviewDevelopment Technician - Software Developer	

Development Operations Engineer - Band N - Counter Terrorism Policing HQ	Application Update	ReviewDevelopment Operations Engineer - Band N - Counter Terrorism Policing HQ	
Development Engineer - Software Developer	Application Update	ReviewDevelopment Engineer - Software Developer	
Development Engineer	Application Update	ReviewDevelopment Engineer	
Development Engineer	Application Update	ReviewDevelopment Engineer	
Developing Threats Team – PC	Application Update	ReviewDeveloping Threats Team – PC	

Dev Ops Engineer (Cloud Platform) - Technology CSC - Police Staff - Counter Terrorism Policing HQ	Application Update	ReviewDev Ops Engineer (Cloud Platform) - Technology CSC - Police Staff - Counter Terrorism Policing HQ	
Detective Sergeant London Region Protected Persons Unit (LRPPU)	Application Update	ReviewDete ctive Sergeant London Region Protected Persons Unit (LRPPU)	
Detective Sergeant Economic Crime - Fraud investigation teams	Application Update	ReviewDete ctive Sergeant Economic Crime - Fraud investigatio n teams	

Detective Sergeant - Image Retrieval Unit	Application Update	ReviewDetective Sergeant - Image Retrieval Unit	
Detective Sergeant - Frontline Policing Delivery Unit - Detective Pathways	Application Update	ReviewDetective Sergeant - Frontline Policing Delivery Unit - Detective Pathways	
Detective Sergeant - Complex Investigation Team (CIT)	Application Update	ReviewDetective Sergeant - Complex Investigation Team (CIT)	
Detective Inspector-Homicide Team	Application Update	ReviewDetective Inspector-Homicide Team	

Detective Inspector – Trident Reactive : Specialist Crime (West Hub)	Application Update	ReviewDetective Inspector – Trident Reactive : Specialist Crime (West Hub)	
Detective Inspector - Trident Reactive South	Application Update	ReviewDetective Inspector - Trident Reactive South	
Detective Inspector - Specialist Investigation Unit - DPS	Application Withdrawn	ReviewDetective Inspector - Specialist Investigation Unit - DPS	
Detective Inspector - Inquiry & Review Support Command (IRSC)	Application Update	ReviewDetective Inspector - Inquiry & Review Support Command (IRSC)	

Detective Inspector - Homicide Teams at Barking	Application Update	ReviewDetective Inspector - Homicide Teams at Barking	
Detective Constable - DASO - Professional Standards	Application Update	ReviewDetective Constable - DASO - Professional Standards	
Designated Detention Officer	Application Update	ReviewDesignated Detention Officer	
Deputy National Coordinator, Protect & Prepare - Supt - Counter Terrorism Policing HQ	Application Update	ReviewDeputy National Coordinator, Protect & Prepare - Supt - Counter Terrorism Policing HQ	
DDaT Operations Manager	Application Update	ReviewDDaT Operations Manager	

DC - Public Order Crime Team	Application Update	ReviewDC - Public Order Crime Team	
Data Quality Management Lead	Application Update	ReviewData Quality Management Lead	
Data Management Officer Indexer - Band E - NDMC - Counter Terrorism Policing HQ	Application Update	ReviewData Management Officer Indexer - Band E - NDMC - Counter Terrorism Policing HQ	
Cyber Unit - DI Protect, Prepare and Prevent	Application Update	ReviewCyber Unit - DI Protect, Prepare and Prevent	

Custody Healthcare Practitioner Open Day Event - Hammersmith Police Station - Thursday 27th June 2024 13:00PM	Registration Update	ReviewCustody Healthcare Practitioner Open Day Event - Hammersmith Police Station - Thursday 27th June 2024 13:00PM	
Custody Healthcare Practitioner Open Day Event - Charing Cross Police Station - Thursday 24th October 2024 13:00PM	Registration Update	ReviewCustody Healthcare Practitioner Open Day Event - Charing Cross Police Station - Thursday 24th October 2024 13:00PM	

Custody Healthcare Practitioner (Registered Nurse / Registered Paramedic)	Application Update	ReviewCustody Healthcare Practitioner (Registered Nurse / Registered Paramedic)	
CTSFO Tactical Advisor	Application Update	ReviewCTSFO Tactical Advisor	
CSC - Offender Management - International Assistance Unit (IAU) Detective Constable	Application Update	ReviewCSC - Offender Management - International Assistance Unit (IAU) Detective Constable	

CSC - Offender Management - Central Orders Team Police Constable	Application Update	ReviewCSC - Offender Management - Central Orders Team Police Constable	
Crime Academy DC - Interview Team	Application Update	ReviewCrime Academy DC - Interview Team	
Covert Admin (COVAD) Deputy Manager	Application Update	ReviewCovert Admin (COVAD) Deputy Manager	
Counter Weapons Threat Team Officer - PC - Counter Terrorism Policing HQ	Application Update	ReviewCounter Weapons Threat Team Officer - PC - Counter Terrorism Policing HQ	

Counter Terrorism Security Advisor (CTSA)	Application Update	ReviewCounter Terrorism Security Advisor (CTSA)	
Counter Terrorism Security Advisor (CTSA)	Application Update	ReviewCounter Terrorism Security Advisor (CTSA)	
Counter Terrorism Police Liaison Officer - DSU - IOPS - Counter Terrorism Policing SO15	Application Withdrawn	ReviewCounter Terrorism Police Liaison Officer - DSU - IOPS - Counter Terrorism Policing SO15	
Correspondence Manager	Application Update	ReviewCorrespondence Manager	
Coroner's Officer Manager	Application Update	ReviewCoroner's Officer Manager	

Contract Lifecycle Support	Application Update	ReviewContract Lifecycle Support	
CONNECT Support Team- User Support Specialist	Application Update	ReviewCONNECT Support Team- User Support Specialist	
Compliance & Assurance Officer - Counter Terrorism Policing HQ	Application Update	ReviewCompliance & Assurance Officer - Counter Terrorism Policing HQ	
Complex Investigation Team (CIT) Police Constable SOIT	Application Update	ReviewComplex Investigation Team (CIT) Police Constable SOIT	

Complex Investigation Team (CIT) Disclosure Support Officer	Application Update	ReviewComplex Investigation Team (CIT) Disclosure Support Officer	
Complex Investigation Team (CIT) Detective Inspector	Application Update	ReviewComplex Investigation Team (CIT) Detective Inspector	
Complex Investigation Team (CIT) Detective Constable	Application Update	ReviewComplex Investigation Team (CIT) Detective Constable	
Complaint Resolution Unit (CRU) - Complaint handler	Application Update	ReviewComplaint Resolution Unit (CRU) - Complaint handler	
Complaint Handler	Application Update	ReviewComplaint Handler	

Communications Manager – Marketing, Campaigns and Internal Communications	Application Update	ReviewCommunications Manager – Marketing, Campaigns and Internal Communications	
Communications Lead – Chief Media Officer	Application Update	ReviewCommunications Lead – Chief Media Officer	
Communication Planning Manager	Application Update	ReviewCommunication Planning Manager	
Commercial Lead Solution Delivery	Application Update	ReviewCommercial Lead Solution Delivery	
Commercial Consultant- Assurance and Risk	Application Update	ReviewCommercial Consultant- Assurance and Risk	

Commercial Consultant	Application Update	ReviewCommercial Consultant	
Commercial Apprentice	Application Update	ReviewCommercial Apprentice	
CJOMS Shift Team Manager	Application Update	ReviewCJOMS Shift Team Manager	
Character Enquiry Centre Team Leader	Application Update	ReviewCharacter Enquiry Centre Team Leader	
Centralised Administration Team Member	Application Update	ReviewCentralised Administration Team Member	
Centralised Admin - Typing Services	Application Update	ReviewCentralised Admin - Typing Services	

CCTV Investigations Assessment/Review - Band D - NDES S3 - SO15	Application Update	ReviewCCTV Investigations Assessment/Review - Band D - NDES S3 - SO15	
Casualty Bureau (CB) Co-ordinator	Application Update	ReviewCasualty Bureau (CB) Co-ordinator	
Case Management Administrator	Application Update	ReviewCase Management Administrator	
Capital Manager	Application Update	ReviewCapital Manager	
Business Change Supervisor	Application Update	ReviewBusiness Change Supervisor	
Business Change Specialist	Application Update	ReviewBusiness Change Specialist	

Business Change Manager - Change - Counter Terrorism Policing HQ	Application Update	ReviewBusiness Change Manager - Change - Counter Terrorism Policing HQ	
Business Change Lead - Change - Counter Terrorism Policing HQ	Application Update	ReviewBusiness Change Lead - Change - Counter Terrorism Policing HQ	
Business Change Communications Specialist	Application Update	ReviewBusiness Change Communications Specialist	
Business Assurance Junior Manager	Application Update	ReviewBusiness Assurance Junior Manager	

Business and Policy Support Officer - Data & Analysis - Counter Terrorism Policing HQ	Application Update	ReviewBusiness and Policy Support Officer - Data & Analysis - Counter Terrorism Policing HQ	
Business Analyst – Strategy, Planning and Performance (SPP) Counter Terrorism Policing HQ	Application Update	ReviewBusiness Analyst – Strategy, Planning and Performance (SPP) Counter Terrorism Policing HQ	
Building Manager	Application Update	ReviewBuilding Manager	
Biometric Intelligence Case Officer - Band D - NDES S6 - SO15	Application Update	ReviewBiometric Intelligence Case Officer - Band D - NDES S6 - SO15	

Beckton Recruitment Event	Registration Update	ReviewBeckton Recruitment Event	
BCU Learning and Development Lead	Application Update	ReviewBCU Learning and Development Lead	
BCU Learning and Development Co-ordinator	Application Update	ReviewBCU Learning and Development Co-ordinator	
Band E Specialist Crime CPS Liaison Team / Met Police Room Central Criminal Court	Application Update	ReviewBand E Specialist Crime CPS Liaison Team / Met Police Room Central Criminal Court	
Audit and Risk Manager - Strategic Planning & Risk	Application Update	ReviewAudit and Risk Manager - Strategic Planning & Risk	

Apprentice Vehicle Mechanical Electrical Trim (M.E.T.) Technician	Application Update	ReviewApprentice Vehicle Mechanical Electrical Trim (M.E.T.) Technician	
Apprentice Motorcycle Technician	Application Update	Review Apprentice Motorcycle Technician	
Anti-Corruption and Abuse (ACAC) Intelligence Bureau.	Application Update	ReviewAnti-Corruption and Abuse (ACAC) Intelligence Bureau.	
Administrative Officer – MO2 - HQ Operations	Application Update	ReviewAdministrative Officer – MO2 - HQ Operations	

202402 - MPS Return Scheme Retired Officers	Application Update	Review202402 - MPS Return Scheme Retired Officers	
202402 - MPS Return Scheme Approaching Retirement	Application Update	Review202402 - MPS Return Scheme Approaching Retirement	
2024-07 Police Constable Degree Apprenticeship (PCDA)	Application Update	Review202407 Police Constable Degree Apprenticeship (PCDA)	
2024-07 Police Constable Degree Apprenticeship (PCDA)	Application Update	Review202407 Police Constable Degree Apprenticeship (PCDA)	

202307 Transferring Officers - Specialist Team	Application Update	Review202307 Transferring Officers - Specialist Team	
202307 Transferring Officers - Neighbourhood Team	Application Update	Review202307 Transferring Officers - Neighbourhood Team	
202305 - Police Community Support Officer (PCSO)	Application Update	Review202305 - Police Community Support Officer (PCSO)	
202305 - Police Community Support Officer (PCSO)	Application Update	Review202305 - Police Community Support Officer (PCSO)	
202207 - Detective Constable Pathway	Application Update	Review202207 - Detective Constable Pathway	

202203 Rejoiner Officers	Application Update	Review202203 Rejoiner Officers	
07-2024 Special Constable (Volunteer Police Constable)	Application Update	Review07-2024 Special Constable (Volunteer Police Constable)	
07-2024 Special Constable (Volunteer Police Constable)	Application Update	Review07-2024 Special Constable (Volunteer Police Constable)	
042024 - DCEP (Detective Constable Entry Programme)	Application Update	Review042024 - DCEP (Detective Constable Entry Programme)	

View cookie policy

© Mayor's Office for Policing and Crime 2016

NIE June Exam – Not Fully Registered

Inbox

metpromotions@police.soprasteria.co.uk

Feb 7,
2025,
6:30 PM

to me

Dear tshingombe

Our records indicate that you have started an expression of interest to sit the NIE Exam in June but you did not fully submit it, if you are still wanting to take the exam please log back into your Oleeo portal and fully submit your expression of interest.

This has to be fully submitted by Monday
17th February 2025 23:55hrs.

Many thanks,

Recruitment Team

SSCL - delivering services in partnership with
the Metropolitan Police Service

HOLMES Incident Manager	6 Mar 2025 23:55 GMT
CATO Administrative Officer	7 Mar 2025 23:55 GMT
National Police Chiefs' Council - Strategic Planning & Performance Analyst	9 Mar 2025 23:55 GMT
Senior Information Assurance Manager	10 Mar 2025 23:55 GMT
MBS Product Lead - User Experience	10 Mar 2025 23:55 GMT
HR Change Manager	10 Mar 2025 23:55 GMT

HR Change Lead	10 Mar 2025 23:55 GMT
Head of Treasury and Financial control	11 Mar 2025 23:55 GMT
Data Protection Lead	11 Mar 2025 23:55 GMT
HR Business Partner (Band S)	12 Mar 2025 23:55 GMT
RPA Developer	13 Mar 2025 23:55 GMT
Database Administrator	13 Mar 2025 23:55 GMT
Parts Technical Advisor	14 Mar 2025 23:55 GMT

Geospatial Data Engineer	14 Mar 2025 23:55 GMT
Business Assurance and Organisation Learning Supervisor - Interventions - CTPHQ	14 Mar 2025 23:55 GMT
Victim Identification Support	14 Mar 2025 23:55 GMT
Domain Lead - Band C - Data & Analysis - Counter Terrorism Policing HQ	17 Mar 2025 23:55 GMT

Information Governance Officer - Band D - Compliance & Assurance - Counter Terrorism Policing HQ	19 Mar 2025 23:55 GMT
Service Delivery Manager - Vehicle Enforcement Team	20 Mar 2025 23:55 GMT
Head of Learning Catalogue	21 Mar 2025 23:55 GMT
Commercial Manager - Property and FM	21 Mar 2025 23:55 GMT
Business Delivery Programme Manager	23 Mar 2025 23:55 GMT

Private Secretary to Assistant Commissioner - Frontline Policing Private Office	23 Mar 2025 23:55 GMT
Complex Investigation Team (CIT) Disclosure Officer	23 Mar 2025 23:55 GMT
Team Leader Onsite Services (North Area)	24 Mar 2025 23:55 GMT
Portfolio Support	24 Mar 2025 23:55 GMT
Team Leader Onsite Services (Central West)	24 Mar 2025 23:55 GMT

Team Leader Onsite Services (South East)	24 Mar 2025 23:55 GMT
Team Leader Onsite Services (North East)	24 Mar 2025 23:55 GMT
Senior Press Officer (Band C)	24 Mar 2025 23:55 GMT
Senior Content, Channels and Engagement Officer	24 Mar 2025 23:55 GMT
Graphic Designer	24 Mar 2025 23:55 GMT
Content, Channels and Engagement Officer	24 Mar 2025 23:55 GMT

National Surveillance Capability Team Policy & Assurance Manager - Band C - Counter Terrorism Policing HQ	24 Mar 2025 23:55 GMT
Press Officer	24 Mar 2025 23:55 GMT
Enabling Services: Team Member (North Area East Cluster)	25 Mar 2025 23:55 GMT
Enabling Services: Team Member (Central Cluster Area)	25 Mar 2025 23:55 GMT

Enabling Services: Team Member (South East-West Cluster)	25 Mar 2025 23:55 GMT
Health & Safety Advisor (Training)	26 Mar 2025 23:55 GMT
Transformation Directorate Business Manager	27 Mar 2025 23:55 GMT
CT Borders - Border Operation Centre (CTBOC) - Technical Lead - Band D - Counter Terrorism policing HQ	28 Mar 2025 23:55 GMT
Head of Innovation - Counter Terrorism Policing HQ	28 Mar 2025 23:55 GMT

Commercial Manager - Property and FM	31 Mar 2025 23:55 BST
07-2024 Special Constable (Volunteer Police Constable)	31 Mar 2025 23:55 BST
2024-07 Police Constable Degree Apprenticeship (PCDA)	31 Mar 2025 23:55 BST
202305 - Police Community Support Officer (PCSO)	31 Mar 2025 23:55 BST
Governance Manager - Strategy, Performance, and Planning - Counter Terrorism Policing HQ	3 Apr 2025 23:55 BST

Senior Project Manager - Technology - Counter Terrorism Policing HQ	4 Apr 2025 23:55 BST	
Custody Healthcare Practitioner (Registered Nurse / Registered Paramedic)	6 May 2025 23:55 BST	
202203 Rejoiner Officers		3
	Closing Date	
Communications Officer (999 & 101)	31 Dec 2025 23:55 GMT	
Volunteer Police Cadet Leader	12 Jan 2026 23:55 G	

Access to HE

Diploma

Specification

Access to HE Diploma

(Policing)

Access to HE Diploma Specification 2024-2025

Diploma overview

The Level 3 Access to HE Diploma is a nationally recognised qualification regulated by the Quality Assurance Agency for Higher Education (QAA) which is designed to provide preparation for study in higher education (HE) in the UK for adults returning to education.

In order the gain the Access to HE Diploma, learners must achieve a total of 60 credits. Of these 60 credits, 45 credits must be achieved at Level 3 from graded subject specific units. Graded units can be awarded at Pass, Merit or Distinction. The remaining 15 credits must be achieved at Level 2 or Level 3 from study skills units which are ungraded.

Diploma details

Diploma title: Access to HE Diploma (Policing)

Learning aim code: 40013182

Validation start date: 1st August 2024

Validation end date: 31st July 2027

SSA sector code:

- Tier 1: 1 - Health, Public Services and Care
- Tier 2: 1.4 – Public services

The Access to HE Diploma (Policing) has been developed in collaboration with the

Metropolitan Police Service. Whilst the Diploma has been developed in collaboration with

the Met Police, centres could work with a local police force to deliver this Diploma.

Diploma aims

The Access to HE Diploma (Policing) offers adult returners a coherent, integrated and

supported year of study through which they will gain the knowledge, awareness, skills and

confidence necessary for successful undergraduate studying in the intended progression

routes for this Diploma. The course aims to provide a balance of essential study skills with

specialist subject knowledge to enable the students to be prepared for the academic and

practical rigours of undergraduate study in HE Policing entry programmes. It must however be

noted that the Access to HE Diploma does not provide guaranteed entry to UK Higher

Education Institutions.

Its primary aims are:

• To provide HE progression opportunities for adults who, because of social, educational

or individual circumstances, do not have the necessary qualifications;Access to HE Diploma Specification 2024-2025

• To give learners a general introduction to the basic concepts, methods, and key areas

of knowledge within the core disciplines taken and offer a coherent and stimulating

framework within which they can broaden their intellectual outlook and make connections between subject areas;

• To help learners to develop and consolidate the various skills required to enable them to cope successfully with the demands of undergraduate study and to become independent, self-directed learners;

• To establish a positive and supportive learning environment within which learners can build their confidence through successful learning and the sharing of their experience;

• To provide the personal, educational support (including preparation for application and interview techniques) needed to facilitate learners pursuing their aims within the framework of the course.

Target learners

• Adults who, because of social, educational or individual circumstances, were unable to participate in or benefit from initial education.

• Adults from groups under-represented in higher education.

• Adults seeking a change of direction because of unemployment or lack of career opportunities in their previous field and who have a demonstrable interest in entering a

Policing career.

Potential progression routes

This Diploma has been designed for progression onto the Police Constable Degree

Apprenticeship and related HE Policing entry degree programmes.

Entry guidance

There are no centrally specified formal requirements for qualifications on entry; however there

is usually the expectation that the learner will have literacy, communication skills and

numeracy at Level 2 or above. For learners wishing to progress to a Police Constable Degree

Apprenticeship, Level 2 English is a pre-requisite with an expectation that Level 2 Functional

Skills Maths will be attained by the end of the first year of the degree apprenticeship.

Advice and guidance

Learners should be aware that degrees undertaken via a specific force will be subject to a

successful application, vetting and offer.

Centres delivering this Diploma must, as part of advice and guidance, make learners aware that

they will not be eligible for the Access to HE Diploma loan waiver for their adult learner loan as

the Police Constable Degree Apprenticeship is not eligible for funding under Student Finance

England. However, learners would be salaried and would not be eligible for any HE fees. Access to HE Diploma Specification

Guided learning hours

The Access to HE Diploma represents 600 notional Guided Learning Hours (GLH) with courses generally delivered in 450 GLH. This may vary between centres and may depend on whether the course is being delivered through blended learning. It is expected a centre delivering the course will clearly outline the intended delivery in terms of total hours and how this is broken down weekly over the period of study.

Diploma resources

The minimum required resources for this Diploma include:

- Access to IT facilities with specialist software as appropriate.
- Access to learning resources and online facilities.
- Access to VLE or other system, such as Microsoft Teams, Google Classroom.
- Access to resources for specialist learner support and reasonable adjustments.
- The same level of facilities and resources should be available at each site where the Diploma is delivered.

Staffing requirements

• Staff delivering, assessing or internally moderating on the Access to HE course must have the professional competence and level of subject expertise necessary to deliver and assess the units available on the Diploma. They should be qualified at Level 4 or above in the named subject, or in a discipline that includes the subject. For example, a tutor with a Social Science degree may be able to teach both Psychology and Sociology.

• Staff should have or be working towards a teaching qualification.

• Staff should have knowledge and understanding of the Access to HE Diploma, including QAA regulations, AVA assessment regulations, the QAA Grading Scheme and the Rules of Combination.

• New staff should be inducted to ensure that they have sufficient information to deliver, assess or internally moderate on the Diploma competently.

• It is desirable that teachers have personal practice experience.

Assessment

Grading Standards

The graded units in an Access to HE Diploma are graded using a scheme which has been designed to accommodate the flexibility of the qualification (it can be applied to all Access to HE Diploma graded units, whatever their subject or structure). A grade of Pass, Merit or

Distinction is awarded for every graded Level 3 unit that a learner completes successfully as

part of an Access to HE Diploma. Grades can only be awarded for graded units which are part of Access to HE Diploma Speci

the Diploma (and conform to the Rules of Combination). There is no overall grade for the

Diploma.

There are 3 grading standards which are applied to **all** graded units:

GS1: Knowledge and Understanding

GS2: Subject Specific Skills

GS3: Transferable Skills

Each grading standard comprises of a set of components and sub-components which describe

types of performance associated with the standard. For each component, there are parallel

statements at merit and distinction, which describe increasingly demanding standards of

achievement. The most appropriate sub-components of the standards are selected when

grading the unit.

For Grading Standard 3: Transferable Skills, all three of the components (a, b and c) must be

used at least once across the Diploma.

For further information can be found here on the OCN London website.

Assessment mechanisms

The Access to HE Diploma assessment mechanism incorporates:

- Assessment tasks which are designed and set by the Centre
- Internal assessment of learner work
- Internal and external moderation of assessment.

There are no additional external assessments for this Diploma.

Recommended methods of assessment

The recommended assessment methods for this Diploma should include a variety of methods which take into consideration the target learners for this Diploma and the appropriateness for the units being assessed. Assessment methods should be valid, reliable, and inclusive and assure equity.

The following assessment methods could be used to assess the units within this Diploma.

Please note, it is expected that at least part of one unit is assessed by formal examination taken under timed conditions.

- Case studies
- Oral presentation

• Practical tasks/demonstrationsAccess to HE Diploma Specification 2024-2025
6
• Question and answer (written and oral)
• Tests/exams with seen or unseen papers
• Tutor observation
• Worksheets
• Written assignments
• Written essays/reports
This is not an exhaustive list and other methods could be selected with agreement from either
OCN London or the Centre Moderator.
Access to HE Diploma Specification 2024-2025
7
Rules of Combination
In order to be awarded the Access to Higher Education Diploma (Policing), learners must
achieve a total of 60 credits comprising:
Credits required from graded academic subject content units at Level 3

45
Credits required from ungraded units at Level 3 or Level 2
15
Total Credits required
60
Learners must also meet the following Rules of Combination:
Rule: Units in
Status
Mandatory
Credits (see
below)
From Optional
Credits
Total
Credits
Study Skills
Ungraded

3 @ L3
12 @ L2 or L3
15
Subject Specific Units
Graded
6 @ L3
39 @ L3
45
In addition:
A learner must achieve a minimum of one 6 or 9 credit unit to achieve the Diploma.
A learner's programme of study can only include a maximum of 30 credits made up from 6 or 9
credit units.
Additional information
Recognition of Prior Learning (RPL)
Overall, the total proportion of credits awarded or exempted through either credit transfer
and/or recognition of prior learning must not exceed 30 credits (that is 50 per cent of the

credits required for the achievement of the Diploma).

Barred Combinations of Units

Where unit content between units overlaps by more than 25% of the learning outcomes this

would represent an excluded combination of units.

Information on barred combinations for this Diploma can be found on page 9. Access to HE Diploma Specification 2024-202

8

Approved Units

Mandatory Units

Unit ID

Unit Name

Level

Credits

CBA782

Reading and Comprehension of Texts

(ungraded)

L3

3

CBA786
Extended Project **(graded)**
L3
6
Study Skills (ungraded)
Unit ID
Unit Name
Level
Credits
CBA847
Essay Writing
L3
3
CBA785
Examination Skills: Preparing for and
Succeeding in an Examination

L3

3

CBA851

Note-taking and Note-making

L3

3

CBB392

Preparation for Higher Education

L3

3

CBB804

Report Writing

L3

3

CBB803

Sourcing and Reading Information

L3

3
CBB805
Speaking and Listening Skills
L3
3
BPM059
Statistics and Probability
L3
3
CBA788
Using Information Technology
L3
3
CBA855
Writing and Delivering Seminar Papers
L3

3
CBA856
Writing Standard English
L3
3
Subject Specific Units (graded)
Policing
Unit ID
Unit Name
Level
Credits
CBB620
Communication Skills in a Police Service
Setting
L3
3
CBB320

Conflict Management within Policing
L3
3
CBB315
Evidence Based Policing
L3
3
CBB316
Intelligence and Information Gathering in Policing
L3
3
CBB621
Introduction to Policing
L3
6

CBB622
Local Policing
L3
6
CBB319
Police Ethics and Values
L3
3
CBB317
Principles of Conducting a Police
Investigation
L3
3Access to HE Diploma Specification 2024-2025
9
Criminology and Law
Unit ID
Unit Name

Level
Credits
CBB348
Arrest, Remand and Bail Procedures
L3
3
CBB347
Aims of Sentencing
L3
3
CBB378
Law and Order in Civil Society
L3
3
CBB623
The Criminal Justice System and Victim Care

L3
3
Sociology
Unit ID
Unit Name
Level
Credits
CBB727
Sociology of Crime and Deviance
L3
3
Barred combinations
There are no barred combinations set for this Diploma.
Access to HE Diploma Specification 2024-2025
10
Guidance and support materials
OCN London devised assignment briefs are available for the following units:

Study skills

- Essay Writing
- Examination Skills: Preparing for and Succeeding in an Examination
- Note-taking and Note-making
- Preparation for Higher Education
- Reading and Comprehension of Texts
- Report Writing
- Sourcing and Reading Information
- Speaking and Listening Skills
- Writing and Delivering Seminar Papers
- Writing Standard English

Subject specific units

- Extended Project
- Sociology of Crime and Deviance

Online learning materials

The following online support materials are available:

• Essay Writing
• Extended Project
• Note-taking and Note-making
• Preparation for Higher Education
• Reading and Comprehension of Texts
• Sourcing and Reading Information
• Writing Standard English
These online learning materials can be used as part of your teaching or an induction to the
course. It is expected that the learners will still receive teaching on these topics and
assignments must be set for them by their tutor and assessed by the centre.
The courses can be accessed via the OCN London website or incorporated into your own VLE or
online delivery systems. If you have any queries, please contact Sarah Francis
(sarah@ocnlondon.org.uk)
All OCN London devised assignment briefs can be found in the Access Centre Area on the
OCN London website (login required).
Further resources and guidance including tutor guidance documents, marketing materials,
forms, templates and checklists can be found in the above area of the website (login may be

required). Access to HE Diploma Specification 2024-2025

11

If you are interested in delivering this Diploma, please contact Michelle Wood (Access to HE

Development Coordinator) at michelle@ocnlondon.org.uk. Access to HE Diploma Specification 2024-2025

12[Type here]

Metropolitan Police Service

Information Pack

COMMUNITY ASSESSOR

Welcome to a changing city, a changing

organisation and a fascinating and exciting

role

[Type here]CONTENTS PAGE

[Type here]

Introduction from the Commissioner

3

Aboutthe Met

5

Executive Structure

11

Job Description

13

Your rewards

15

EligibilityCriteria

16

What to do next

18INTRODUCTION FROM THE COMMISSIONER

I am looking for someone outstanding to join my team who can help us manage the daily challenges London poses, and who can also drive the change necessary for the Met to keep pace with this vibrant city. London is a fantastic place and I have always been incredibly proud to serve the capital. It is a diverse, growing and ever-changing city with national impact and international reach.

How the Met operates has changed significantly in recent years, achieving a step change in effectiveness, efficiency and confidence. But the scale of our ambition for the future is even greater. It has to be.

There are many challenges facing policing. I have no doubt the Met can meet them all – to transform, to exploit the opportunities of the digital age, to get the best from our people and most importantly to make London the safest it can be.

The Mayor has set out his priorities in his Police and Crime Plan – a bold and challenging agenda with a focus on priorities. My particular focus is to bear down on violence in all its forms, protecting the vulnerable and the security of our city. I want us to become even closer to our communities, building confidence and trust.

One of my central aims for the Met is that we are a modern police service, but with the best of policing's traditional values at our core. To do that we need every single part of the force to be well led, every officer and staff member to feel supported and to have the right equipment to help them serve London.

I want all our people to believe in the Met and the tangible difference they make every day across the city so that we can become even better at keeping London safe. I want the public

to believe in us too and so I want us to be more transparent about what we do on their

behalf.INTRODUCTION FROM THE COMMISSIONER

Our values of courage, compassion, integrity and professionalism remain at the heart of

everything we do. My commitment to you is to lead the Met in a way that respects and nurtures

these very traditional values but which also puts us at the forefront of modern policing and

maintains Scotland Yard's well-earned international reputation.

This information pack will give you further insight into the role, and the qualities and experience

we are looking for.

I very much hope you will be inspired by this opportunity to serve with the Met.

Cressida Dick CommissionerABOUT THE MET

Founded by Sir Robert Peel in 1829, the Metropolitan Police Service (the Met) is one of the

oldest police services in the world. From the beginning, the purpose of the Met has been to

serve and protect the people of London by providing a professional police service. This remains

our purpose.

Our vision is to make London the safest global city, a city in which people are free to be

themselves, express themselves and flourish. We strive to earn the trust and confidence of every community and take pride in the quality of our service so that people love, respect and are proud of London's Metropolitan Police.

The Met is responsible for maintaining the peace and is accountable in law for the exercise of policing powers, and to the Mayor's Office for Policing and Crime (MOPAC) for the delivery of efficient and effective policing, management of resources and expenditure. At all times the Commissioner and her officers remain operationally independent, in the service of the public.

The Met 'New Scotland Yard' is internationally recognised for its history, law enforcement and skills in fighting crime, however a constantly changing city needs an accessible police service which reflects and understands the people it serves. It needs an effective police service equipped for the 21st century with a visible service which every day continues to earn the trust and confidence of Londoners.

Today, the Met is made up of more than 39,000 officers and staff, plus thousands of volunteers; we are one of the largest employers in London and the South East of England. The territory we serve covers 620 square miles and is home to over 8.6 million people. The Met is the UK's largest police service and has 25% of the total police budget for England and Wales.

We're proud that the Met is seen as a world leader in policing. The 'Scotland Yard' brand is known around the world as a symbol of quality investigation and traditional values of policing.

Thanks to this reputation, our services are highly sought after, either through using our officers and staff in operational matters or by training others and giving them the opportunity to learn from our experiences.ABOUT THE MET

LONDON: THE AMAZING GLOBAL CITY WE POLICE

London is unique: 'the world under one roof'.

Its ever-changing population is set to grow towards 9.2 million by 2020 and exceed 10 million the following decade. It is probably one of themost diverse cities in the world. The complexities of policing a city on this scale are huge. A seat of Parliamentary, Royal and Diplomatic power, London is a centre for protest, for criminality, for transport.

Londoners tend to be younger than the rest of the UK, more than three million of us were born abroad, just under half of which arrived in the UK less than 10 years ago.

London is also the world's most popular business and travel destination, receiving 31.5 million Visits in 2015, 12.9 million from the UK. It is a global city, recognised around the world, economically, politically, financially and creatively. London's greatness comes from its openness to

the world, and this in turn has helped build world-renowned institutions which have preserved its safety and stability.

There are over 200 languages spoken in London, and around 40% of the population is Black or Minority Ethnic (BAME). These numbers are predicted to grow further as the city expands and develops as an international centre.

Of the six largest world faiths, almost four million Christians and onemillion Muslims live in London, and Buddhism, Hinduism, Judaism and Sikhism each have more than 80,000 followers in the capital.

London's population swells due to an influx of commuters during the day and tourists throughout the year - in greater volumes than anywhere else in the UK.

London is one of the safest global cities in the world already. Nevertheless, criminality within London is on a more prevalent and serious level than other cities and communities across England & Wales. Crime in the capital is often connected to organised criminality and national and international networks of offending. London has, throughout our lifetime, been a place that terrorists want to attack.

This creates a unique policing environment. Everyone joining us needs the ability to deliver outstanding policing to the communities of London.ABOUT THE MET

WE HAVE A HIGHLY AMBITIOUS TRANSFORMATION AGENDA

Our transformation programme

Like many public bodies, we work with constrained resources, increasing demand and a changing environment that require us to make policing in London ever more effective. Recognising the challenges and the opportunities to improve our services, we are currently in the midst of one of the biggest transformation programmes of any public sector organisation.

Our **Transformation Portfolio** aims to deliver transformation right across our functions and departments, to modernise the force as a whole, and keep our resources focused on priority areas, providing an effective and efficient service to all Londoners.

In the past twelve months we have delivered:

· **A more visible neighbourhood presence**, with about 1,700 dedicated officers whose sole focus is to respond to the issues that matter to local communities (two police constables (PCs) as Dedicated Ward Officers (DWOs), and one Police Community Support Officer (PCSO) in all 629 London wards). These officers are tackling local priorities and anti-social behaviour, identifying people vulnerable to, or at risk of becoming involved in crime, and solving local issues.

· A strengthened local police. By regrouping a small number of boroughs to deliver core local policing functions (neighbourhoods, safeguarding, response and investigation) across borough boundaries, we can integrate and enhance our capability, and improve the safeguarding of vulnerable people with more officers dedicated to prevention. Management costs will reduce, which means we can maximise the availability of officers on the frontline. People, buildings, technology and fleet currently in one borough will be shared across a Basic Command Unit (BCU), making it easier to provide resources in line with each local area's peaks in demand. In addition, we have opened up access to a police career through direct entry superintendents, inspectors and detectives, attracting a diverse pool of applicants who may not have otherwise considered a career in policing.

· Significant enhancements to our service. Our new website offers relevant local information and prevention advice. It is includes online crime reporting capability: 11 per cent of crimes are now reported online. A new Telephone and Digital Investigation Unit complements this, reducing demand on our response teams, allowing them to focus their efforts more effectively. Body Worn Video (BWV) cameras were rolled out to over 22,000 officers, more than any other police service in the world. By being the first British police

service to share footage digitally with the criminal justice service, we have improved security, reduced the demand on officer time and saved £3.5 million per year in operating costs. Complaints and investigations can become more evidence-based with supporting BWV material. ABOUT THE MET

· Smarter Working bringing a significant range of savings and qualitative benefits, including improved morale, officer visibility and service effectiveness and efficiency. As a result of the rollout of 30,000 tablet and mobile devices, we have the ability over time to support our officers with better applications so they spend more time visibly assisting the public and less time in our buildings; we also expect to be able to better serve the public, with our officers having access to the right information at the time when they need it.

We have a clear roadmap that sets out our transformation plans to 2020. We have reviewed our processes and capabilities, our organisational, technological and digital strengths and weaknesses; and are constantly assessing future demand and current gaps to identify where change is necessary, where investments are required, and where benefits can be realised.

We need to make further savings, whilst continuing to improve our operational effectiveness and efficiency in the face of increasing overall demand, higher expectations from the public and the

added complexity of a digital age.

Technology and estate transformation are some of the key enablers of that change, but organisational culture and learning, and good information management are also vital to make it a success. ABOUT THE MET

For London…

A modern, transformed and more **efficient Met** will **Protect London** by investing more ofits time on the areasof greatestthreat, risk and harm;

We will make **every community safer** through our new neighbourhood policing service anda stronger focuson safeguardingtoprotectthe mostvulnerable.

For Our People…

We will provide **real time information** to keep them safe and manage risk, and provide **professional support** so they can concentrate on their job;

We will deliver a **digital service** from contact to court to help meet demand, and trust in them to do their job well and have good professional judgement so their time is spent on activities that have the most impact.CORPORATE PRIORITIES

Our mission is to keep London safe for everyone

To achieve this, we will:

Focus on what matters most to Londoners

Violent crime tops the public's concerns and tackling it is our top priority. This includes terrorism, knife and gun crime, sexual offending, domestic abuse and safeguarding vulnerable people from predatory behaviour.

Mobilise partners and the public

We know that safety requires action and intervention beyond the police service. We will work with partners and communities to help keep them safe and support them in preventing crime.

We will work harder to earn the trust of more young people and ethnic minority communities.

Achieve the best outcomes in the pursuit of justice and in the support of victims

We have a fundamental responsibility to uphold the rule of law and to ensure that victims receive the best possible outcome. We will do this by catching offenders and by ensuring victims of crime receive both justice and the support they need from us and our partners.

As an organisation, we want to lead 21st century policing and:

Seize the opportunities of data and digital tech to become a world leader in policing

We want to harness data and use advanced technologies to our advantage in the pursuit of criminals, rising to the challenge of a fast-moving data-driven digital age. We will make information and insight more accessible internally, and externally, to support evidence-based decisions and promote public confidence.

We will strive to enhance our global reputation for excellence and expertise in policing.11BACKGROUND

12

The MPS Assessment Centre deals with the interviewing and assessment for all posts where we recruit in large volumes. This involves assessments for new Police Officers, Police Community Support Officers, Special Constables, Designated Detention Officers, as well as the recruitment of new Detectives.

Every role will have a slightly different assessment process, based on job specifications. This will range from an interview and written test, to a half-day assessment including interview, role plays, interactive and video based scenarios.

We assess both Police Officers and Police Community Support Officers to the National assessment standard. This National standard is a Home Office regulation for Police Officers, so every force in the country must recruit to this level. Only assessors that have been trained to the National Standard, may undertake this kind of assessment. The training course is delivered over

a 4 day period and takes place at our Assessment Centre premises in West Brompton, London.

Primarily, this is where our Community Assessors are used.

With the introduction in 2018 of a refreshed police Recruitment process called Day One, which incorporates IT for candidates and assessors use, all assessors will be required to be comfortable with the use of technology in the assessment process. All training is provided on using the tech, as well as the assessment material.

After successful completion of the Community Assessor training course, assessors will then be offered work on a causal basis. Assessment activity will fluctuate dependent on the Recruitment activity taking place and their availability. It is a flexible role and is designed to enable assessors the ability to work assessing around other responsibilities. Based on demand community assessors may assess from between 2-3 days a week to a couple of days a month.

It is possible that once a Community Assessor has gained experience in the National method of assessment, that if they are suitable, further training may be offered to participate in other kinds of interviews (for example Detectives and Police Community Support Officers). There is also the opportunity to develop further in the role, with the Quality Assurance role, or delivering training.

It is important we have a team of professionally trained assessors to support our recruitment assessments. Bringing with you a variety of different experience and to reflect the diversity of

the communities we serve.COMMUNITY ASSESSORS -PERFORMANCE FRAMEWORK

13

Job title: Community Assessor

Location: West Brompton

Responsible to: Assessment Centre Manager

The post holder is ultimately responsible to the Head of Examinations & Assessment at the College of Policing. However, on a day-to-day basis, post holders are responsible to the Metropolitan Police Service assessment delivery lead.

The primary purpose of the post is to make objective assessments of the performance and competence of candidates during their assessment day. This will involve assessment of candidates through a variety of activities, involving interviewing, written, interactive and video based exercises. You will be required to use immersive technology for some assessments.

Please note, on occasion some assessments may be performed at other locations in London, in which case advance notice will be given.

Tasks and Responsibilities:

· Establish effective working relationships with the assessment team, stakeholders and

candidates. It is essential to provide a first class candidate experience.

· Set up assessment room at start and end of assessment day, ensuring correct material is available for assessment process.

· Ensure readiness at the appointed time in the exercise room before the start of each assessment. Timekeeping is extremely important, ensuring prompt arrival at start of day and adherence to the assessment timetable during the assessments

· IT competency is a requirement. Training will be provided, but you must be willing to use a tablet for recording assessment notes.

· Carry out assessments to evaluate, making assessment decisions on the competence or performance of the candidate. Assess objectively using the observe, record, classify and evaluate (ORCE) performance using behavioural statements, scalars and grades correctly

· Observe candidate language and behaviour and written ability in respect of set competencies Record any instances of inappropriate language or behaviour by candidates in accordance with training.

· If undertaking role acting, Learn background material, lines, questions, probes and the behavioural checklist specific to the exercise

· Maintain records of assessment activities to meet internal or national verification standards.

· Attend and contribute to Assessor engagement briefings/meetings

· Attend regular refresher training to maintain competency and to assist with Continuous Professional Development14

COMMUNITY ASSESSORS -PERFORMANCE FRAMEWORK

Skills and Abilities:

· An ability to work as part of a high performing team

· Highly developed interpersonal skills

· Ability to communicate to a high level in both written and spoken English

· Prepared to deliver and receive constructive feedback

· Sound judgement and the ability to assess others objectively, fairly and consistently

· High levels of concentration and stamina

· Ability to monitor own performance and undertake self-development

· Flexible approach to work, prepared to work alone or as a team member Confidence to take responsibility for decisions.

Continuing Professional Development (CPD)

· Maintain competence in own area of assessment subject matter expertise, including knowledge and understanding of assessments, relevant legislation, College of Policing

· Participate in networking opportunities, and contribute to assessment engagement meeting by reflecting upon existing practice and sharing learning with peers in order to inform and improve policy, processes and practice.

· Maintain and enhance knowledge and understanding of new approaches to assessment.

· Complete all mandatory training as require.

· Enhance knowledge by undertaking training for difference recruitment assessment processes.

· Embrace development opportunities to progress as a Quality Assurer or Training for Assessment delivery.YOUR REWARDS

Community Assessors and paid £150 per day (prior to tax and NI) for assessing. Additionally reasonably travel expenses (i.e. train/bus fare) can be claimed for attendance at an assessment event. Please note that this is for Transport for London Zones 1-6 only.

This is an excellent opportunity to have an involvement in the recruitment of new Police

Constables who will be serving Londoners.ELIGIBILITY CRITERIA

16

For further information regarding the eligibility criteria for joining the Met, please visit the Met

Careers website or the information contained in the application.

The Met is committed to safeguarding the welfare of children and vulnerable adults. As part of

these safeguards, the MPS adopts a consistent and thorough process of safe recruitment in order

to ensure that all MPS staff and volunteers are suitable.

Posts that involve a high level of contact with children and vulnerable adults will additionally

require a Criminal Record Bureau (CRB) check.ELIGIBILITY CRITERIA

17

Your application form will be initially sifted against MPS criteria such asconvictions

and residency.

· Following the initial sift your application will be assessed against the rolecriteria.

· If successful at this stage we will contact you regarding an interview date. Youwill receive a

minimum of 7 days' notice. If you are unsuccessful at this stage we will also write to you and

advise you ofthis.

· The interview will be a competency-based interview and questions will be posed around the

criteria for the role in question, as set outin the advert and information pack.

· If successful at interview we will send you an initial offer of employment which sets

out what happens next.

· If unsuccessfulwewill alsoadvise youinwritingbutwill beunableto offer feedback.

Please note any correspondence received from us will be via e-mail and sent to the

address you provide on your application form.WHAT TO DO NEXT

Please submit your completed online application by the advert closing date.

For general enquiries please visit www.metpolicecareers.co.uk, which includes an 'Answering

Your Questions' section or contact the Recruitment Team on 01633 632500.

· The recruitment process is thorough and consequently can be quite lengthy.

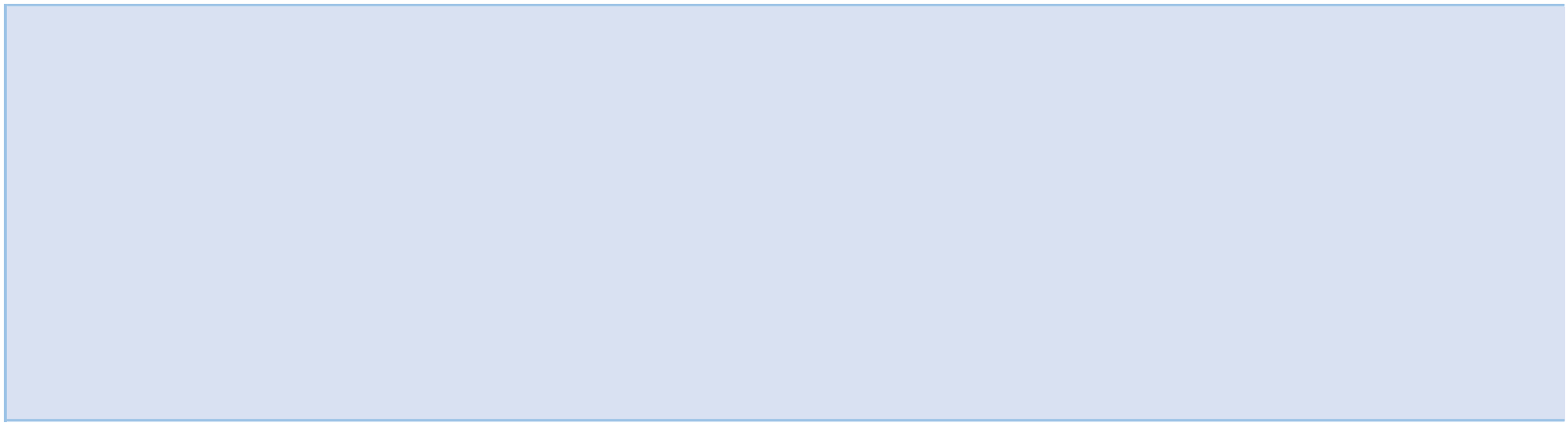
· Shortlisting and interviews will be based on the criteria listed.

· Until an offer of appointment is confirmed in writing, you should not assume your

DataRights@met.police.uk	12:05 PM (1 hour ago)
to me	

Thank you for the email and contacting the MPS "Data Office - Data Rights Unit datarights@met.police.uk". Our office is open Monday to Friday only, and this department is closed on bank holidays.

Please note that we receive a large volume of emails through this mailbox, and all emails are dealt within date order. So it may not be possible to respond to you by return.
Therefore we ask you to please be patient and allow us some time to respond to you, before you contact us again. We will get back to you as soon as we can and we thank you again for your patience.



Please note that our response may come from the email address DataRightsDONOTREPLY@met.police.uk . To ensure that our responses are not sent to your spam folder, please add this email address to your safe senders list.

The following types of applications are processed within this mailbox;

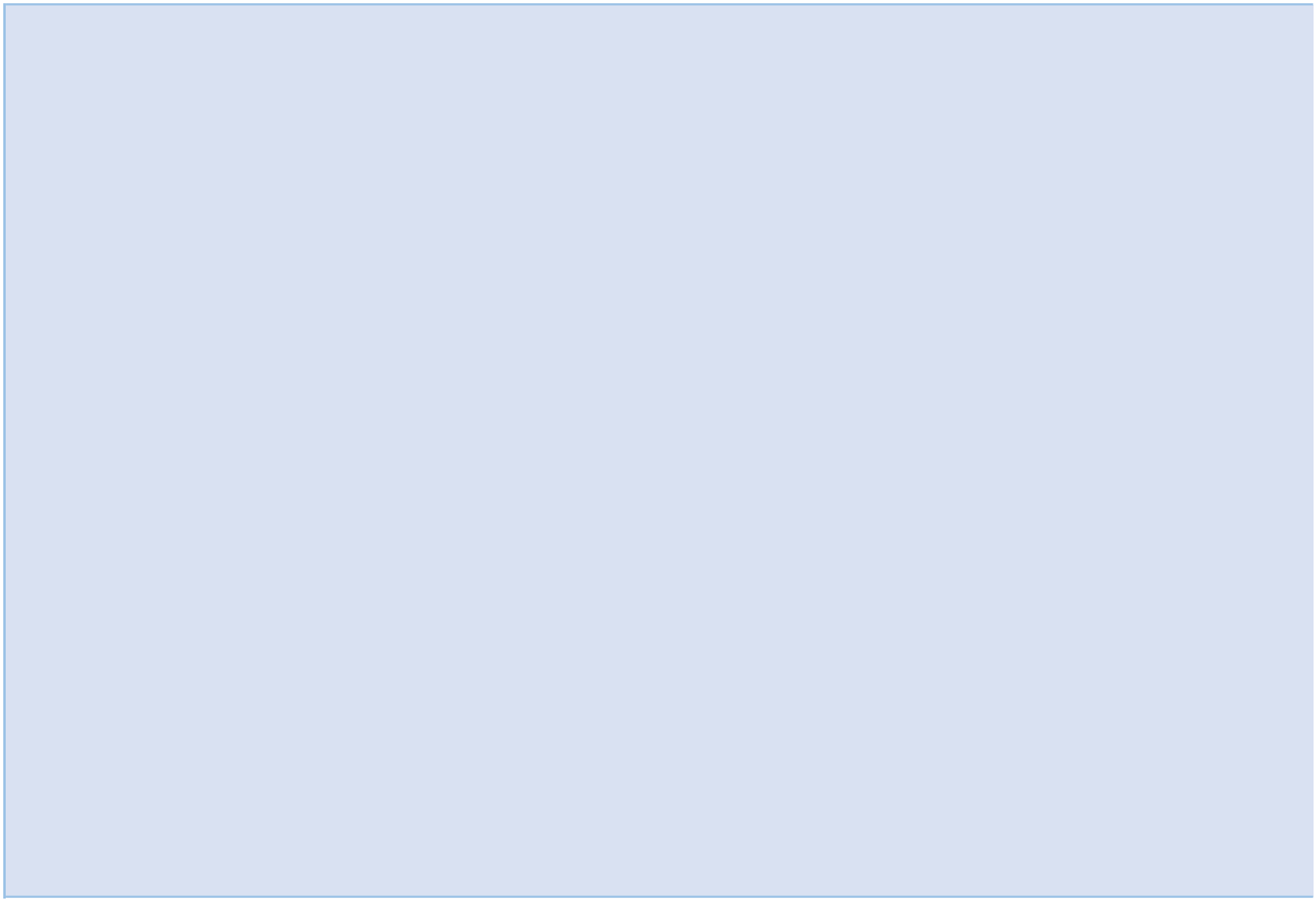
· Right of Access Requests (Formerly Subject Access Requests)

· Freedom of Information Act Requests

· National Guidance on Data Sharing for National Police Chiefs' Council (NPCC) in respect of Association of British Insurers (ABI) v.2.2

· Right to Erasure and Right to Rectification Requests

· Requests under the Environmental Information Regulations 2000



If you have any other request/application that fall outside the above criteria, please understand that these do not fall under the scope of our services, and we will be unable to help you. Consequently those emails will be disregarded by us and no response will be sent to you. ***Therefore, it is advisable you redirect your request to the appropriate unit***. *Please see below contact detail that may help you re-direct your request to the appropriate unit.*

Traffic related request	· Any queries relating to Automated Speed or Red light offences with a reference number that commences 0013 please email SafetyCameraManagers@met.pnn.police.uk

	· Traffic Offence Reports or Officer issued tickets or offences with a reference number that commences 0012, 0015, 0016 or 0018 please email: fixedpenaltynoticeenquiries@met.pnn.police.uk

	For all other traffic related matters, please use the below forms and contact details on it (Met Prosecution, Po box 510, DA15 0BQ);

	· Form 518A - Request for Traffic Case Reference number (met.police.uk)

	· Form 518 - Request for Police Collision Reports and Third Party Details in Road Traffic Collisions (met.police.uk)

	· Form 519 - Request for Police Collision Reports and Third Party Details in Road Traffic Collisions (met.police.uk)

	· Form 521 - Request for Police Collision Reports and Third Party Details in Road Traffic Collisions (met.police.uk)

	· Form 522 - Request for Officer Interviews in Road Traffic Collisions (met.police.uk)

ACRO (list of conviction and caution, PNC information)	https://www.acro.police.uk/s/acro-services/subject-access

The information held on the PNC includes, but is not limited to details of arrests, impending prosecutions, convictions, non-convictions such as penalty notices, cautions, final warnings, reprimands, individuals disqualified from driving and information relating to the issue of firearms certificates.	

Bail to Return enquiries	Any enquiries for updates regarding case progression, investigation or bail be directed to the investigation officer or the BCU in the case Contact us | Metropolitan Police. Please do not contact the custody suites or the data rights directly.	

DBS Applications	Any enquiries for updates regarding submitted application, please contact customerservices@dbs.gov.uk or DBS customer services, PO Box 3961, Royal Wootton Bassett , SN4 4HF	
Request for Finger Prints	https://www.met.police.uk/rqo/request/fp/af/your-fingerprints	

National Guidance on Data Sharing for National Police Chiefs' Council (NPCC) in respect of Association of British Insurers (ABI) v.2.2	**Please note only insurance requests from or on behalf of ABI members will be considered.** Applications forms will require the ABI representative contact name and email address, prior to acceptance. *Please await our response whilst our dedicated team work through the applications as quickly as possible.*	

Request information under Clare's Law	This scheme enables the police to release information about any previous history of violence or abuse a person might have Request information under Clare's Law: Make a Domestic Violence Disclosure Scheme (DVDS) application | Metropolitan Police	

Request information under Sarah's Law (Child Sex Offender Disclosure Scheme)	Sarah's Law (Child Sex Offender Disclosure Scheme) | Metropolitan Police

Third party information required for other purposes (including MIB request's)	If you require third party information for reasons aside from legal proceedings, you will need to request this from the Commander of the Borough police where the incident occurred. MPS Contact Us.	

Validation of reports	Requests to validate crime reference numbers or limited particulars will not be dealt with by this department without the appropriate application documents and consent from the Data Subject. If we receive such a request we will file these emails away without sending out a response. You should send your enquiry to the appropriate unit via MPS Contact Us.

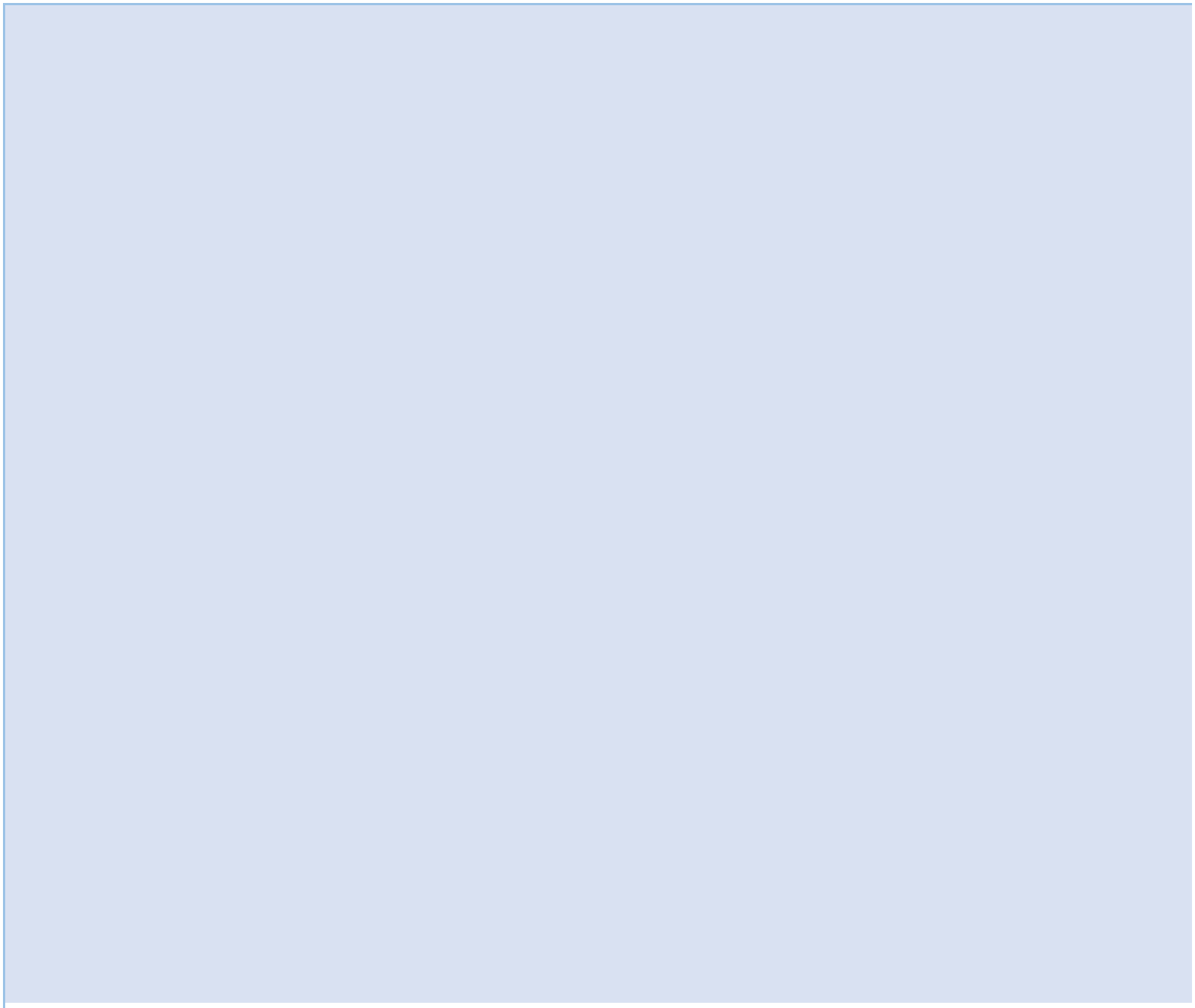
Useful contact details:

If it's related to any other matter please visit
www.met.police.uk

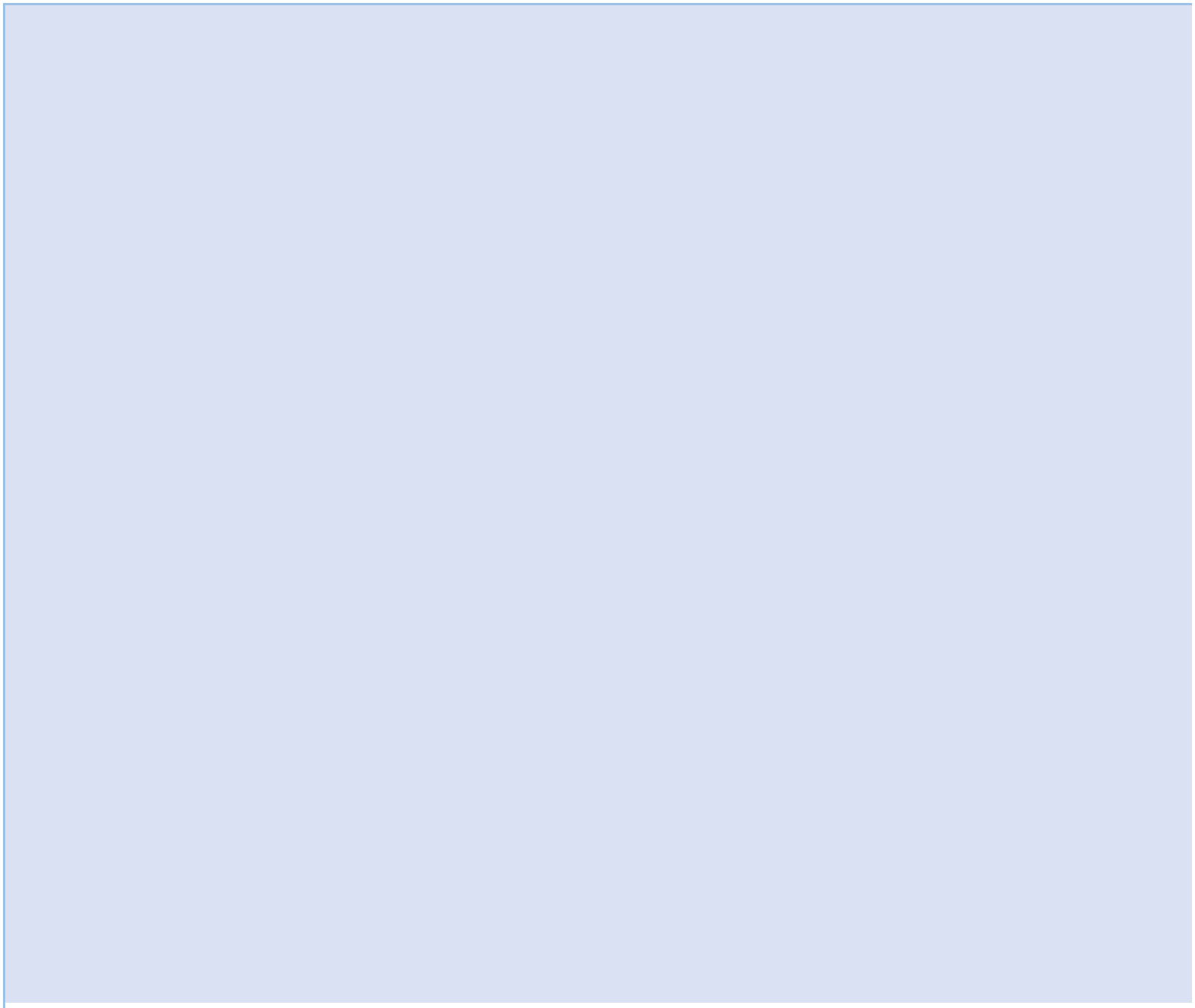
Information required for Family Court Proceedings	If you require information for use in Family Court Proceedings, you would need to contact the MPS Directorate of Legal Services (DLS) - DLSMailbox-LegalSupportDisclosure@met.police.uk. For any other purpose, please visit I'd like to request disclosure for family court proceedings about myself | Metropolitan Police	

Information required for other legal proceedings	If a court case is anticipated, you should request the information you require under Schedule 2, Part 1, Paragraph 5(3) of the Data Protection Act 2018 to the Commander of the Borough police (at your local police station) where the incident occurred

To reach an officer, another unit, the local Borough Command Unit/Police station or other.	Contact us | Metropolitan Police
To make a complaint	Complaints | Metropolitan Police



This email and any attachments are solely for the intended recipient and may be confidential. If you have received this email in error, please notify the sender and delete it from your system. Do not use, copy or disclose the information contained in this email or in any attachment without the permission of the sender. Metropolitan Police Service (MPS) communication systems are monitored to the extent permitted by law and any email and/or attachments may be read by monitoring staff. Only specified personnel are authorised to conclude binding agreements on behalf of the MPS by email and no responsibility is accepted for unauthorised agreements reached with other personnel. While reasonable precautions have been taken to ensure no viruses are present in this email, its security and that of any attachments cannot be guaranteed.



NOTICE - This email and any attachments are solely for the intended recipient and may be confidential. If you have received this email in error, please notify the sender and delete it from your system. Do not use, copy or disclose the information contained in this email or in any attachment without the permission of the sender. Metropolitan Police Service (MPS) communication systems are monitored to the extent permitted by law and any email and/or attachments may be read by monitoring staff. Only specified personnel are authorised to conclude binding agreements on behalf of the MPS by email and no responsibility is accepted for unauthorised agreements reached with other personnel. While reasonable precautions have been taken to ensure no viruses are present in this email, its security and that of any attachments cannot be guaranteed.

REPUBLIC OF SOUTH AFRICA

e Department of Justice and Constitutional Development (DOJ&CD

IN THE HIGH COURT OF SOUTH AFRICA

boysen court office

Appeal Case Number:

Ja 37/19,, ja 2461/15,;

A Quo Case Number:

Urn number case : 4702024FCV001046

1

In the matter between

Tshingombe tshitadi fiston APPELLANT

and

Elizabeth lerumu ccma labour / RESPONDENT

Department of labour

Department government

Department education high education dbe

Saqa

Department transport

Head argument , leave to appeal

Referral

Delivered: was handed down electronically by circulation to the parties' representatives

Civil procedure – final protection order – Domestic Violence Act 116 of 1998 – Scope of protection order – Definition of dom

Violence work place

1] This appeal is against the finding and order section 6 of the Domestic Violence Act, 116 of 1998 (the Act). The respond

[2] The grounds of appeal are that the magistrate erred in the following respects. First, by erroneously finding that the re

[4] The respondent's application for a protection order was

[5] The respondent alleged in her founding affidavit.

[6] By way of background, the respondent 12 years old when he was approximately 15 years old.

6.My Protection Order Cases

Your DOJ Online Protection Order Applications : Create a new Protection Order Application

Cases I created

Case Name	Service Type	Case Type	Created At	Case Status
Tshingombe Tshitadi	Domestic Violence	Protection Order	Jul 22 2024 8:51PM	Screen Application

My Protection Order List

No records to display.

My Safety Monitoring Notice Application List

Tshingombe Tshitadi	Domestic Violence	Protection Order	Nov 25 2024 5:44PM	Screen Application

DOJONLINEEST202408061672	Deceased Estate	ICT/System related	Awaiting DHA verification

DOJONLINEEST202407221507	Deceased Estate	ICT/System related	Awaiting DHA verification

DOJONLINEEST202407221506	Deceased Estate	ICT/System related	Deceased Estate Application Rework

DOJONLINEEST202407221505	Deceased Estate	ICT/System related	Case Status

Showing records from 1 to 5 of 4

Cases I created

Case Name	Service Type	Case Type	Created At	Case Status
tshingombe tshitadi	Civil Law	Civil	Nov 19 2024 5:55PM	Incomplete
tshingombe tshitadi	Civil Law	Civil	Aug 9 2024 2:20PM	Pending Document Review
tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 9:17PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 4:23PM	Screen Application

tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 4:41AM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 4:36AM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 4:32AM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 5 2024 4:26AM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 4 2024 8:27PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 4 2024 8:21PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 4 2024 8:03PM	Incomplete
tshingombe tshitadi	Civil Law	Civil	Aug 4 2024 7:51PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Aug 4 2024 5:57PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Jul 21 2024 12:20PM	Screen Application
tshingombe tshitadi	Civil Law	Civil	Jul 21 2024 12:18PM	Incomplete

Re: referral.. Appeal council labour order index pleading, booking granted filing record transcript appointment court probono event..Meeting. employments, development justice land outcome,rigth justice labour mandatory

*Referral: revised.

Outcome review agreement

Nomination granted function posted graduated review finalize record job career low issue license permit

- chancellor policy awareness;

Referral notice :re - appeal

-

Introduction :

Background : review re appeal formal ,master form filing form instructional completed

Check list, affidavit answer sock evidence, affidavit evidence, complain form investigate answer evidence .unopposed.. Opposite sock council referral ,provisional bank response evidence balance onus. Unopposed bank fund ..petition unoppsite learner council chancellor unoppsite , government unoppsite proof service ,proof registered mail unopposed .evidence clear ,, enforcement low unopposed event ..

- * content files :

- summary

1. Section :

Introduction

1.Background

1.1Judgement leave appeal : jr 2461/15,attach Ccma record ,,

Pg -

1.2 . Judgment leave judgment appeal

:index of pleadings , affidavit proof ..

1.3 . Notice of set down in order : check list :
notice opposition , answers: affidavit:

, reviews.

1.4. letter security security :

2.section :

Introduction :

Background

2.1.index of pleadings, noticed: compliance :
Ccma file notice compliance outcome labour
,

2.2. rescission ruling : guide

2.3 .application for leave to appeal: media .

3.Section :

Introduction :

Background :

3.1 .application for leave to appeal :

4.Section :

4.1in the commission for concilliation :

Variation of ruling , arbitration award

4.2 leave to appeal

- 5.section : application heads of argument .

5.1 letter : dear ,affidavit

.6 section :

registration, form process :

6.1 psira application regulation check application
Certificate occurent book.
6.2 register regulation nogada agreement job psira report individual Ccma ..:
6.3. pratice manual of the labour RSA ,ccm module course .:
6.4 labour ICBL ,check ,:permit work check saqa ,coid ,council job
- nomination form social work
-uif insurance labour ,application form appeal form :
- coid : application form instruction completed. ..regulation labour OSHA .nominate form, award ,electrical compliance form check regulation :
Rules
7.section :

7.1 report application head skill: development sale

7.2 record bookkeeping shop mall..:

7.3 .cna shopprite record extra saving: reward .office save office cna casebook .parking cts return cash back job employment document wallet appointment .. company relia hr ..experimental n.textbook .application tax.

8. Section :

8.1 .skill development sasseta :

,seta regulation , assessessment

sasseta ,

certificate form skill registration

Scie bono assessessment.

8.2.translate copy dr Congo ,saqa French English low attestation ,certificate diplomat , birthday document ..inpp

Saqa check list :

- 8.3.home affairs appeal check :

_____

Conte file JA 37/19

-appeal ,Estes issue file

Re - appeal/ re- estate

- section 1.

1.1 section 1.: order court notice petition:

.1.2 case 297/11/2024-16 points .:

1.3 application for protection Cass :

.1.4. justice complains bargaining levies

Ordered ,compliance ,

contravention form investigation ammandement :107,163.7 nbcpss .

1.5. justice complains bargaining levies ordered :.

1.6. bargaining referal : jr 2462

1.7. index pleading :

1.8.order court petition :

1.9. affidavit in support of service by registered:

1.10 .Proof affidavit :

1.11. Sherif complain : sherrif affidavit

- section 2:

2.1.Affidavit in section criminal procedy

- 2.2.complain form : details employer

2.3. PFA complain form : detail

2.4. complain form details

2.5. affidavit in section criminel procedure ..

3.Section :

-3. File appeal record file move :

3.1 pleading index retrieview file:

3.2 refers in the labour ..

3.3. master court documents files:

3.4 notice appeal department,:

3.5. referral.

- 3.6honorable justice labour and: registray labour :.

3.7 notice leave appeal :

.section 4

4.1 section

4.1. notice of motion : petition for leave appeal .

4.2 . submission.: transform industrial

4.3 application for judgement leave to appeal head argument.
4.4 master court jurisdiction index pleading rigty low legacy litigat in execution of sole property.:
4.5 .bid close : argument record retrieview files .head argument leave to appeal judge filing retrieved in support affidavit..
4.6 . agreements judgement order order petition agreemy ..
Section 5
- 5.1Ccma process in Limon ,con ARB , rescission review case audit ,case details eventy statist case file case audit audit award ..
- 5.2 requested for arbitrat LRA form 7.13

Section 6.

6.1. skill e legit reviews guide .

6.2. labour court and Ccma rules ,

6.3 complaint agy Sherriff central / ,(019/1#/119.3 copy policy

6.4 . Labour court and ccmz rules ..

6.5.skill development legisy reviews guide ..

Section .

-7. labour chairing disciplinary psira

7.1 department of labour register skill merseta topic. Peace ..

7.2. labour on labour appeal jhb force ..

7.3 To the director general : lab justice defense force .:

Enforcement low ruling award notice compagny

7.4. development section bargaining :

Sector report office drawing engineering trade skill manufacture related process claim

7.5. directive order enforcement:

-referal :

* Section

- background review :

Occured in labour court and labour appeal court psira complain exempted investigation security private industrial investigate award ruling rescission and record transcription provisional court execution rwiten sherrif labour granted review skill development

Investigation trial court evidence low burn award and outcome certificate council private sector ,saps and safety in development justice protection order issue Manuel and humain rigth intelligence service trial court point investigate agreement national council bargaining private security and provide fund trial license term outcome ,cipic sars intellectual property and revenue pension fund sector , building council agreement justice labour policy procedure hr gift insurance and compensation dol building evidence high court summons notice motion on leave to appeal refuse granted success power arrested debator creditor appeal high court and labour court appeal leave levy skill magistration ,,rigth humain legislator mendator security office and police office power attorney government framework regulator .trial cipic deregistered compagny private and private sector industrial ,revenue sector amendment business ,notice motion security docket saps docket system unity power arrest warrant arrested claim small business license labour appeal court and development justice master court .labour taxation matter

Parking mall court guard order security attorney and tenure order security bargaining security low tendered close order total claim 210500 rand claim in high court and labour appeal court guard court bargaing consolidation process before to protect compagny in process before to keep process of client bargaining agreement government minister granted if judge process with file and put security challenges to keep protect process judge must grant amount of money is cost in labour bargaing and Ccma ,, compagny low enforcement gaek must pay post registered mail ,,in case of continue assessment in case library high court and labour appeal court open file book casebook retrieview must granted review copyrith in case government notice open file investigation site government legal paralegal warden safety saps must granted review in case warden search ambassador for more job car guard minister said and safety homes affairs must granted review for pliagiarism and copy of job in case minister education high and land reform open supplieb open award outcome for review more skill development must granted sassa uif coid

Trial victim labour witness labour claim security in the minister deputy , bill Amandment low .trial investigation claim contrevention .cash center bank stateme

In the labour court of South africA

In the labour appeal court of South Africa

In the developmt justice court master court

In high court magistrate

Held in Johannesburg

- in the matter between .: case No jr 2461/15

Ja 37/19

Referral :

NO| Description of document. | Page no

_____
____

-1 index notices : 1-4

Introduction :

Background

-2 notice of motion: 1-9

-3 affidavit in support of application 5-9.

-4 Proof of service : 10-14

- . Notice of set down :

-5 . Notice in term of rule: 7A 1-2

-6. Records : 3-35

-7.recording transcription: 35-43

-8. Notice judgement leave appeal :43-49

-9.affidavit registered mail in support:49-49

- 10reason notice notice of motion : 50-55

-11. Notice of opposition unopposed: 55-56

- 12. Application for leave to appeal head argument 56-141

- 13. Notice proof of service contract ruling record :282-300

-14. notice proof of service skill development record (300-582)

-15. Notice outcome record gov appeal agreements (582-672)

_____

No| description of documents | page no

- 1 notice of motion petition for leave to appeal : 1-36.

- 2 notice of motion submission for application : 36-80

- 3 Proof of service records ..

-4 .affidavit in support of application register : 80-82

-5.affidavit in terms of sect 44(1) complain : 82-95.

-6. Notice of motion order petion petion orders : 95-102

-7.notice of record order transcript : 102-104

-8 notice application for leave to appeal unnoppsite : 104-138

-9. Notice proof of service contractor close :138-200

- 10 notice proof of service applicant execution : 200-338

-11. Notice proof of service : agreement contract : 338-416

- 12 notice notice affidavit record answer investigation:-416-458

- 13. Notice of of gov notion motion outcome : 458-488

- 14. Notice of contract ccm close inlimine : 788-

- 15. Notice of skill of development agree application ..

Master of the high court service :

- 1.court service :civil law

Name | service type | case type | created |
case status | urn | manage •

-urn : 1042024CIV004539

- 1042024CIV004511

-112024CIV00013

-112024CIV00012

-112024CIV00011

-112024CIV00010

-112024CIV00009

-112024CIV00008

-112024CIV00007

-112024CIV00006

-112024CIV00005

- 2. Maintenance:

-3 protection order :

- 4 status tracking :

-5.Query management :

- my query list :

DOJONLINEEST 202312211 deceased estate ICT / system related , application

202312212 deceased estate .master file related query information ,, appointment booking ...

--------_____

Document

-Notice motion summon

-

ACTIVISM ROW STANDS FOR SOCIAL JUSTICE ORGANISATIONS & SOCIAL MOVEMENTS 2025

Inbox

Google Forms <forms-receipts-noreply@google.com>

Fri, Jan 31, 7:13 PM (2 days ago)

to me

Thanks for filling out ACTIVISM ROW STANDS FOR SOCIAL JUSTICE ORGANISATIONS & SOCIAL MOVEMENTS 2025

Here's what was received.

ACTIVISM ROW STANDS FOR SOCIAL JUSTICE ORGANISATIONS & SOCIAL MOVEMENTS 2025

Applications close on 07 March 2025, or When applications have reached capacity.
Email *
tshingombefiston@gmail.com
ORGANISATION DETAILS
What is the name of your organisation? *
Tshingombe Ccma labour court DOJ/ ass police engineering
Name of the contact person or representative *
Tshingombe
Contact Number of representative *
725298946
Email Address of representative *
tshingombefiston@gmail.com
Briefly describe the work of your organisation. (Less than 75 words) *
Ccma labour court tshingombe vs security police officer rigth government mendator land provide fund .granted review
Telephone Number for the organisation *
725298946
Email address or the organisation *
tshingombefiston@gmail.com
Website URL *
https:// tshingombe.com
Please upload a high resolution logo of your organisation *
Submitted files

	3formsubmission-request-ip-licence-mip-327-24-0100-000 sale force emet tshingombe - tshingombe fiston.pdf
What festival theme would your organisation best fit under? *	
✓	Racial justice and anti-racism
✓	Economic and social rights,
✓	Environmental justice
✓	LGBTQIA+ rights
✓	The right to a fair trial and access to justice.

✓	The rights of refugees and migrants
✓	Women's rights and gender equality
✓	Children's rights
✓	The rights with disabili
	Other:

HUMAN RIGHTS FESTIVAL STAND REQUIREMENTS

What size stand would you like? *

3 x 3 Stand (R1000 - Includes table; 2 chairs and signage)

Do you require an electric plug point? This is an additional R150. *

	Yes
✓	No

Create your own Google Form

Does this form look suspicious? Report

t

Protection of Personal Information Act (POPI Act)

Welcome to the Protection of Personal Information Act (often called the POPI Act or POPIA) in the form of a website so ever

You can read a summary of POPIA, attend a POPI workshop, read POPIA judgments and cases, get a POPIA compliance frame

Please note that we are not the Information Regulator who regulates POPIA. You can visit their website or email them.

The commencement date of POPIA

It was 1 July 2020 and the one year grace period to comply ended on 30 June 2021. Parliament assented to POPIA on 19 No

Topics related to the POPI Act

- · POPIA regulations
- · Application and commencement
- · Unique to South Africa
- · Access to information
- · Actions to take first
- · Big data
- · Breach notification
- · Children
- · Code of conduct
- · Consent
- · Contract
- · Cookies
- · Data subject rights
- · Direct marketing
- · Information officer
- · Information regulator
- · Managing operator relationships
- · Mapping activities
- · Media
- · Obligations
- · Operator
- · Opt out

· Personal Information
· Policies
· POPI Act
· POPIA
· Purpose
· Quick wins
· Reasonably practicable
· Records management
· Records of processing activities
· Research
· Responsible party
· Right to be forgotten
· Risks of non-compliance
· Securing information
· The conditions

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) – AN EMPLOYER'S PERSPECTIVE

by Jan Truter | May 11, 2021 | 0 comments

Purposes of the Act

The Protection of Personal Information Act of 2013 (POPIA) follows the example of similar, quite onerous legislation in the E

Personal information is defined as information that relates to a natural or juristic person (such as a company). This includes

Some personal information is designated as special information, that is, personal information relating to information concer

Processing refers to the handling of personal information, e.g., the collection, recording, storing, updating or distribution th

Impact on the employment relationship

In the employment context POPIA covers all personal and special personal information that an employer (referred to as a 're

- Employers must appoint an information officer who needs to be registered with the Regulator.
- Personal Information may, subject to certain exceptions, only be collected by an employer directly from the emplo
- Employees must be informed why the information must be collected (purpose) and who the intended recipients c
- Personal Information may only be processed for an explicit, specific and lawful purpose (such as the conclusion of
- Personal information may not be kept for longer than necessary to achieve the purpose for which it was collected
- Personal Information must be distributed in a way that is compatible with the purpose for which it was collected.
- Personal Information may not be distributed to other third parties, e.g., for instance for marketing purposes.
- Employers must take reasonable steps to ensure that the information collected is accurate, up to date and comple
- Employers must ensure that the personal information is protected against risks of loss, damage, destruction or un

- Employees must also be allowed to access their personal information and can demand that the information be co

When may personal information be processed?

The Act provides for limited use of employee data in some cases, i.e.:

- If the employee consents;
- When processing is necessary for purposes of employment, e.g. details of banking accounts in order to be able to
- If the employer has a legal obligation to perform processing, e.g., for tax purposes;
- To protect a legitimate interest of the employee's, e.g., collecting personal information required by a retirement f
- If it is necessary to pursue the legitimate interests of the employer or a third party, e.g., doing a check on the crim

Special personal information

Additional protections apply to special personal information. This may only be processed if :

- The processing is carried out with the consent of the employee (written consent is not required but is advisable);
- The processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- The processing is necessary to comply with an obligation of international public law;
- The processing is necessary for historical, statistical or research purposes if this serves a public interest (e.g., disea
- The information has deliberately been made public by the employee, e.g. on social media.

What about medical testing?

Medical testing of employees can yield particularly sensitive information about employees. The Act mirrors section 23 of the

Rights of employees in respect of their personal information

Employees have the right to be notified by their employer that their personal information will be collected or has been acce

Consequences of non-compliance

The Act provides that employers can be fined between R1 million and R10 million, or imprisonment for one to ten years dep

Some practical recommendations

Employers would be well advised to attend to the following:

1. Appoint an information officer or assign someone to take on this responsibility. It goes without saying that this pe
2. Develop a privacy policy or data privacy statement that:
    - mentions the circumstances under which personal information may be collected and what may it be used
    - states what kinds of personal information may be collected; to which internal and external recipients or ca
    - states whether the information may be distributed or stored outside of the country's borders; and
    - includes a general description of the of information security measures (such as fire walls) that will be impl
3. Review or develop standard clauses on data protection in employment contracts and provide for employee conse
4. Conduct an audit in respect of personal information currently being held, where such information is being held ar
5. Raise awareness within the organisation of the implications of the Act and the importance of protecting privacy.

6. Report data breaches to the Information Regulator and employees concerned.
7. Do not share any personal information unless it would be permissible to do so in terms of the Act.

Implementation

Employers need to be compliant by no later than 30 June 2021, when the Act will come fully into effect. An organisation's In

Conclusion

While the Act seems very long-winded and makes for difficult reading, it should not be too difficult for employers to comply

With the emergence of the Johnny Depp and Amber Heard Trial saga, domestic violence has never been more prevalent. So

Be advised that an Interim Protection Order or a Final Protection Order only comes into effect when personally served upon

DOMESTIC VIOLENCE PROTECTION ORDER:

A Protection Order is an order issued by a court ordering a person with whom one has or has had a domestic relationship (t

HARRASMENT PROTECTION ORDER:

A Protection Order is an order issued by a court ordering a person with whom one is not in a domestic relationship i.e., a ne

DO I QUALIFY FOR A DOMESTIC VIOLENCE PROTECTION ORDER?

The conditions for a Protection Order in terms of domestic/gender base violence are as follows:

1. There must be a pattern of abuse i.e., repetitive actions.
2. It must be a form of domestic violence which includes but are not limited to:
    1. Physical violence,
    2. Sexual violence,
    3. Financial abuse, and
    4. Emotional/verbal violence.
1. The order may also prohibit the Respondent from:
    1. enlisting the help of another person to commit any such act;
    2. entering a residence shared by a complainant and the Respondent or a specified part of the shared reside
    3. financially threatening the victim by making monetary relief available to the victim.

DO I QUALIFY FOR A HARRASMENT PROTECTION ORDER?

1. No pattern is needed, and a first offence can be sufficient for a Harassment Order.
2. No relationship is required, and it can be against someone you don't even know.
3. No violence is required.
4. It must be a form of harassment which includes but are not limited to:

1. messaging,
2. unwanted packages,
3. letters, psychological harm,
4. physical harm, and
5. financial harm.

1. The order may also prohibit the Respondent from:
    1. To cease and desists with his/her stalking, harassing behaviour or enlisting the help of another person to c

HOW DO I OBTAIN A PROTECTION ORDER?

The following procedure has been established to obtain a Protection Order:

1. OBTAINING AND COMPLETING:

For a Domestic Violence Application, one will need to obtain a Domestic Violence Act Form 2 and complete the Form 2 as accurate as

For a Harassment Protection Application, one will need to obtain the Protection against Harassment Act Form 2 and complete the For

Any victim of domestic/gender-based violence is advised to first register a criminal case at their local police station. In doing

Requesting a protection order doesn't mean that you're laying a charge against your abuser. However, if you're a victim of a

2. DISCRETION OF THE COURT TO GRANT AN INTERIM ORDER:

Before obtaining a protection order, you need to apply for an interim protection order first. A magistrate court will consider

3. SERVICE UPON RESPONDENT:

An interim protection order will be granted and will then be served to the Respondent. The interim order specifies the date

4. RESPONSE BY THE RESPONDENT:

The Respondent will now have an opportunity to file and serve an answering affidavit upon the complainant and the Court i

5. GRANTING A FINAL ORDER:

A court proceeding or hearing of evidence will determine whether a final protection order should be granted.

6. CONSEQUENCES FOR THE RESPONDENT:

Consequences for the Respondent if he/she violates the conditions of the final protection order. If your abuser breaches, or

If your abuser is found guilty of breaking the conditions of a protection order in a criminal case, he or she can be fined or se

To be successful in obtaining a Protection Order, one must note the dates, time and place where the harassment or abuse t

Thus, it is important to call a qualified attorney to advise you on your prospects of succe

The SAPS offers careers in various fields. If you join the SAPS you can either become a police official or a civilian employe

Career Opportunities:

Police Act

Job Title	Remuneration Level	Location	Closing Date
	No post		

Information

t

tshingombe fiston <tshingombefiston@gmail.com> May 29, 2025, 10:37 AM (1 day ago)

to me

Station: Hillbrow (Gauteng)

<< Back

Phone: 011-4886511
Fax: 011-4886798
Email: nevhuhulwias@saps.gov.za

Physical Address:	**Postal Address:**
01 Claredon Place	Private Bag X7
Hillbrow	Hillbrow
Johannesburg	Johannesburg
2038	2038

LATITUDE: -26.18823 **LONGITUDE:** 28.04464

Additional contact numbers:

- Community Service Centre

  Contact nr: 011-4886 517

- Detective Service

  Contact nr: 011-4886 854, 082 7789 655

- Station Commander

Contact nr:	011-4886742, 082 8545 394

- Switchboard

Contact nr:	011-4886511

- Visible Policing

Contact nr:	011-4886853, 071 6756 080

LOCATION: Detective Officer: Investigation Team B: Economic Crimes,

Hillbrow, Gauteng (2 Posts)

REFERENCES: GP 49/3/17

Generic Requirements:

- Competency in the post-specific functions of the post;
- Be in possession of a Senior Certificate (Grade 12)
- Be proficient in at least two official languages, of which one must be English;
- Must be a SA Citizen.
- Be in possession of at least a valid light motor vehicle driver's licence;
- Must have no criminal record or pending criminal or departmental cases;
- Applicants will be subjected to a vetting process which will include security screening and fingerprint verification;
- Relevant courses in the field of the post may be an advantage;
- An applicable NQF 6 qualification and 2 years relevant experience in the field of the post, of which 1 year should be on supervisory level.

Core Functions:

- Control and supervise Detective Service: Economic Crime investigation responsibilities and activities.

- Align Detective Service: Economic Crime activities with cluster/station's strategic direction.
- Ensure quality administrative control and data/documentation integrity of detective Service: Economic Crime.
- Ensure that relevant crime information contained in the case docket is reflected on the Crime Administration System (CAS)

GENERAL

- Only the official application form (available on the SAPS website and at SAPS recruitment offices) will be accepted. The Z83 previously utilized will no longer be accepted. All instruction on the application form must be adhered to. Failure to do so may result in the rejection of the application.
- The post particulars and reference number of the post must be correctly specified on the application form.
- A comprehensive Curriculum Vitae must be submitted together with the application form.
- Certified copies of an applicant's ID document, Senior Certificate and all

educational qualifications obtained, service certificates of previous

employers stating the occupation, proof of relevant experience in the field

of the post and motor vehicle driver's licence.

- The copies must be correctly certified on the copy itself, not at the back.

The certification must not be older than three months.

- Qualifications and driver's licences submitted will be subjected to

verification checking with the relevant institutions. The South African Police Service will verify the residential address of applicants and conduct

reference checks.

- Appointments will be made in terms of the South African Police Service

Act, 1995.

- Applicants appointed under the Police Service Act will be subjected to

undergo a lateral entry training programme art a SAPS training

institution, where applicable.

- Applications must be delivered timeously. Late applications will not be

accepted or considered.

- The closing date for all applications is **30 April 2017.**

- If a candidate is short-listed, it can be expected of him/her to undergo a personal interview as well as a practical assessment.
- Reference checking will be conducted on all short listed applicants,
- **Short-listed candidates for appointment to certain identified posts, will be vetted in terms of the Criminal Law (Sexual Offences and related Matters) Amendment Act, 2007 (Act No 32 of 2007) and the children's Act, 2005 (Act No 38 of 2005). A candidate, whose particulars appear in either the National Register of Sex Offenders or Part B of the Child Protection Register, will be disqualified from appointment to the post.**
- All short-listed candidates will be subjected to fingerprint screening.
- Correspondence will be conducted with successful candidates only. If you have not been contacted within 3 months after the closing date of this advertisement, please accept that your application was unsuccessful.
- The South African Police Service is under no obligation to fill a post after advertisement thereof.

- The SAPS application forms can be obtained from any SAPS Recruitment

Office within the South African Police Service.

Applications must be posted to:

Lt Col Henning

Private Bag X57

Braamfontein

Johannesburg

2017

Hand delivered to:

Lt Col Henning

SAPS Provincial Head Office

16 Empire Road

Parktown

Johannesburg

2017

Enquiries can be directed to:

Lt Col Henning

Tel: 011 274 7913

LOCATION: Sub Section Commander: Shifts, Hillbrow, Gauteng

REFERENCES: GP 38/3/17

Generic Requirements:

- Competency in the post-specific functions of the post;
- Be in possession of a Senior Certificate (Grade 12)
- Be proficient in at least two official languages, of which one must be English;
- Must be a SA Citizen.
- Be in possession of at least a valid light motor vehicle driver's licence;
- Must have no criminal record or pending criminal or departmental cases;
- Applicants will be subjected to a vetting process which will include security screening and fingerprint verification;
- Relevant courses in the field of the post may be an advantage;

- An applicable NQF 6 qualification and 3 years relevant experience in the field of the post, of which 2 years should be on supervisory level.

Core Functions:

- Manage and control crime prevention and crime combatting functions of sector policing to create a safe and secure Station Area.
- Plan and coordinate crime prevention projects or operations.
- Manage the CSC activities at the Station.
- Ensure that crime prevention initiatives take place in accordance with identified crime trends.
- Obtain crime information from CIO and plan operations accordingly.
- Advice the Station Commander on unrest in the Station precinct.
- Manage Sector Policing and ensure that Sector vehicles operate within designated Sector.
- Mange all physical and human resources allocated to Shift.

GENERAL

- Only the official application form (available on the SAPS website and at

SAPS recruitment offices) will be accepted. The Z83 previously utilized

will no longer be accepted. All instruction on the application form must be

adhered to. Failure to do so may result in the rejection of the application.

- The post particulars and reference number of the post must be correctly

specified on the application form.

- A comprehensive Curriculum Vitae must be submitted together with the

application form.

- Certified copies of an applicant's ID document, Senior Certificate and all

educational qualifications obtained, service certificates of previous

employers stating the occupation, proof of relevant experience in the field

of the post and motor vehicle driver’s licence.

- The copies must be correctly certified on the copy itself, not at the back.

The certification must not be older than three months. • Qualifications and driver’s licences submitted will be subjected to

verification checking with the relevant institutions. The South African

Police Service will verify the residential address of applicants and conduct

reference checks.

- Appointments will be made in terms of the South African Police Service Act, 1995.
- Applicants appointed under the Police Service Act will be subjected to undergo a lateral entry training programme art a SAPS training institution, where applicable.
- Applications must be delivered timeously. Late applications will not be accepted or considered.
- The closing date for all applications is **30 April 2017.**
- If a candidate is short-listed, it can be expected of him/her to undergo a personal interview as well as a practical assessment.
- Reference checking will be conducted on all short listed applicants,
- **Short-listed candidates for appointment to certain identified posts, will be vetted in terms of the Criminal Law (Sexual Offences and related Matters) Amendment Act, 2007 (Act No 32 of 2007) and the children's Act, 2005 (Act No 38 of 2005). A candidate,**

whose particulars appear in either the National Register of Sex

Offenders or Part B of the Child Protection Register, will be

disqualified from appointment to the post.

- All short-listed candidates will be subjected to fingerprint screening.
- Correspondence will be conducted with successful candidates only. If you have not been contacted within 3 months after the closing date of this advertisement, please accept that your application was unsuccessful.
- The South African Police Service is under no obligation to fill a post after advertisement thereof.
- The SAPS application forms can be obtained from any SAPS Recruitment Office within the South African Police Service.

Applications must be posted to:

Lt Col Henning

Private Bag X57

Braamfontein

Johannesburg

2017

Hand delivered to:

-2--3-

Lt Col Henning

SAPS Provincial Head Office

16 Empire Road

Parktown

Johannesburg

2017

Enquiries can be directed to:

Lt Col Henning

Tel: 011 274 7913

Apply for a Domestic Violence protection order

What is domestic violence?

According to the Domestic Violence Act No. 116 of 1998 it is:

- any form of abuse which includes physical, sexual, emotional, psychological or economic harassment
- damage to property

- stalking
- entry into a person's property without their consent
- any other abusive or controlling behavior where such a conduct causes harm or may cause harm to your health, safety, or well being

If these forms of abuse are happening to you or to anyone you know, you can apply for a protection order. A domestic violence protection order is a document issued by the court which prevents the abuser from:

- committing an act of domestic violence
- enlisting the help of another person to commit any such act
- entering a residence shared by the complainant and the respondent
- entering a specified part of such a shared residence
- entering the complainant’s residence
- entering the complainant’s place of employment
- preventing the complainant who ordinarily lives or lived in a shared residence from entering or remaining in the shared residence or a specified part of the shared residence or

UTH AFRICAN POLICE SERVICE

CATION FOR APPOINTMENT IN AN ADVERTISED POSTS

SOUTH AFRICAN
POLICE SERVICE

THIS FORM IS ONLY APPLICABLE TO POSTS ADVERTISED INTERNALLY AND/OR EXTERNALLY, ON SALARY LEVELS 2 – 12 (both Public Service Act and South African Police Service Act)				
SURNAME	INITIALS	tsh		

Post for which you apply (as indicated in the advertisement):

THIS IS THE POST REFERENCE NUMBER THAT WILL BE REGISTERED

POST REFERENCE/ REFERENCE NUMBER		POST PARTICULARS	

Γ EMPLOYER / POST THAT YOU OCCUPY AND PROVINCE / DIVISION:

EMPLOYER		POST	post
PROVINCE	Gauteng		
DID YOU APPLY FOR ANY OTHER POST IN THIS ADVERTISEMENT?			YES
IF YES, SPECIFIY THE POST NUMBERS:			

INSTRUCTIONS

-

Enquiries can be directed to the contact person mentioned in the advertisement.	
✏	Only the official application form, which can be obtained from the SAPS website: www.saps.gov.za, will be accepted.
✏	All instructions on this application form must be adhered to. Failure to do so may result in the rejection of the application.
✏	**This form must be properly completed and be signed and dated by the applicant.** Applicants must endorse their initials and surname at the bottom of every page in the space provided.
✏	**This application form must be completed in block letters (handwritten or typed)**
✏	**The post particulars and number of the post must be correctly specified on the application form.**
✏	**A separate original application form and CV must be submitted for each post you apply for. Copies will not be accepted.**
✏	**The CV must contain full particulars of**:
· all boards on which an applicant serves;	
· remunerative work outside the public service;	

· current employment and other business interests; and	
· career promotions, appointments, career developments, career history, current studies and	qualifications.
✏	**An applicant must also attach to every application copies of the following:**
· ID document;	
· valid motor vehicle driver's license;	
· All educational qualifications obtained, Senior Certificate, Degree / Diploma certificates of all post school educational qualifications obtained (academic records and / or statement of results only do not suffice); and	
· Service certificates of previous employers stating the post occupied, must also be submitted.	
✏	**Applications must be delivered timeously. Late applications will not be considered.** It is the responsibility of the applicant to ensure that the application has been received **on or before the closing date and time of the advertisement** (please note that **in the event that an application is posted, it must be reached at the indicated office before or on the closing date and time specified in the advertisement). If you send your application by Courier, send it to our door address.**

✏	**Applications which do not meet the above-mentioned requirements may be rejected.**
✏	**Correspondence will be conducted with successful candidates only.**
✏	Verification of qualifications will be done and the appointment will be subjected to confirmation of the qualifications.
✏	Short-listed candidates will be interviewed only on the date and time specified by the relevant selection committee.
✏	In filling the above post, an applicant whose appointment will promote representivity may receive preference.
✏	The South African Police Service is not under any obligation to fill a post after it has been advertised.

✏	Although the post is advertised, the National Commissioner may withdraw the post from the advertisement, re-advertise the post or fill the post by transferring a person at the same level where this is deemed to be in interest of service delivery.	
✏	The appointment of the successful applicant will come into effect on the first day of the month following the date on which the National Commissioner approved the appointment.	

PERSAL NUMBER (currently in SAPS, SANDF or another Public Service Department)	
SURNAME	
FIRST NAMES	
IDENTITY NUMBER	
DATE OF BIRTH	**10/11/1982**
PRESENT RANK / POSITION	
ARE YOU A SOUTH AFRICAN CITIZEN?	
DATE APPOINTED IN PRESENT RANK / POSITION	

POSTAL ADDRESS			
1030 /20 percy street			
POSTAL CODE			
TELEPONE NUMBER (HOME)			
TELEPHONE NUMBER (WORK)			
CELL			
E-MAIL			
AFRICAN	M.>>	F	
MARITAL STATUS			
DRIVERS LICENCE	YES		
ARE YOU PHYSICALLY DISABLED (SPECIFY)			
ARE YOU IN GOOD HEALTH?			
PHYSICALLY	YES		
IF YOU ANSWER TO ANY OF THE ABOVE IS NO, SPECIFY			
ANY OTHER COMMENT(S) CONCERNING YOUR HEALTH			
DO YOU HAVE ANY VISIBLE TATTOO?			
IF YES, SPECIFY (APPEARANCE / ON WHICH PART OF THE BODY)			
HAVE YOU EVER BEEN DISCHARGED FROM A PREVIOUS EMPLOYER OR POST?			
IF YES, SPECIFY THE FOLLOWING REASON (SELECT ONE WITH AN X)			
RETRENCHMENT	MISCONDUCT	MEDICAL UNFITNESS	SEVERANGE P

DATE OF TERMINATION:	
EMPLOYER:	
IN INSTANCE OF VOLUNTARILY RESIGNATION, WAS THERE A DISCIPLINARY CASE PENDING?	
IF YES ABOVE, PROVIDE DETAILS IN A SEPARATE SHEET	
ARE YOU A MEMBER OF ANY COUNCIL, BOARD OR PRIVATE ENTITY?	
IF YES, SPECIFY,sapu ,,	
ARE YOU INVOLVED IN ANY OUTSIDE BUSINESS, ACTIVITIES OR HAVE ANY INTERESTS WHICH MAY CONFLICT OR IS LIKELY TO CONFLICT WITH THE EX YOU BE THE SUCCESSFUL CANDIDATE FOR THIS POST?	
IF YES, SPECIFY	
Nogada sa security ,,, conflict	
ARE YOU CONDUCTING BUSINESS WITH THE STATE OR ARE YOU A DIRECTOR OF A PUBLIC OR PRIVATE COMPANY CONDUCTING BUSINESS WITH THE STATE?	
IF YES, PROVIDE DETAILS	
Tshingombe engineering //ccma	
IN THE EVENT THAT YOU ARE EMPLOYED IN THE PUBLIC SERVICE, WILL YOU BE PREPARED TO IMMEDIATELY RELINQUISH SUCH BUSINESS INTEREST?	
HAVE YOU BEEN FOUND GUILTY OF ANY CRIMINAL OFFENCE	
IF YES SPECIFY FOLLOWING:	
CASE NUMBER: NAME OF STATION:…… CAS……./MONTH……./YEAR……..	
TYPE OF OFFENCE: (e.g. assault)	
SENTENCE IMPOSED (MARK WITH AN X):	
IMPRISONMENT	SUSPENDED
	Period: From …….. (date)
PERIOD: …… (e.g. 2 YEARS)	To …….. (date)
HAVE YOU EVER BEEN GOUND GUILTY IN A DISCIPLINARY MATTER?	
IF YES, SPECIFY THE FOLLOWING>>ccma nogada case labour court , high court doj	
MISCONDUCT (e.g.) absence without leave)	
Ccma labour doj ,, dismissal award ruling outcom judgment in cort	
SANCTION IMPOSED:	
DATE OF SANCTION:	
ARE YOU A RESPONDENT IN AN INTERIM OR FINAL PROTECTION ORDER IN TERMS OF THE DOMESTIC VIOLENCE ACT, 1998 (ACT NO 116 OF 1998) OR 2011)?	
IF YES, SPECIFY	

Court orde doj boysen .. dismissal order reason found affidavit

DOES YOUR PARTICULARS APPEAR IN THE REGISTER REFERRED TO IN CHAPTER 7, PART 2 OF THE CHILDREN'S ACT, 2005 (ACT NO 38 OF 2005) OR THE NATIONAL SEX OFFENDERS REGISTER [SECTION 42 OF THE CRIMINAL LAW (SEXUAL OFFENCES AND RELATED MATTERS) AMENDMENT ACT, 2007 (ACT NO 32 OF 2007)]? IF YES, PARTICULARS MUST BE ATTACHED	**YES**	**NO>>>**
IF YES, SPECIFY		

HAVE YOU EVER BEEN REFERRED TO A PSYCHIATRIC HOSPITAL IN TERMS OF SECTION 77(6) / OR FOUND NOT TO HAVE HAD THE NECESSARY CRIMINAL CAPACITY AND REFERRED TO A PSYCHIATRIC HOSPITAL IN TERMS OF SECTION 78(6) OF THE CRIMINAL PROCEDURE ACT, 1977 (ACT NO 51 OF 1977)? IF YES, PARTICULARS MUST BE ATTACHED	**YES**	**NO>>>**
IF YES, SPECIFY		

B. CAREER PROMOTIONS / APPOINTMENTS

YEAR	PROMOTION / APPOINTMENT *(*INDICATE POST TITLE AND NAME OF EMPLOYER)*
2010	Security office car guard cta , compagny nogada sa/saps service
2015	Security officer , shaka shile
2015	Seurity section one /cambridge food policy safey
2020	St peace colllege /assessment police //saqa dhet nated
2022	Security engineering sarb , policy

2023	Police met uk on line /detective inspector
2024	Microsoft engineering senior ,security police research
2024	Psira security/ sasseta , inspector
2024	Scheineder security pysical
2024	Eskom/ city power , physical security
2024	Sars/ policy physical

C. CAREER DEVELOPMENT (TRAINING: COURSES)

PLEASE COMPLETE IN FULL

YEAR		COURSE PARTICULARS	DURATION OF TRAINING / COURSES (eg. 3 days / 2 weeks, etc.)
20120	St peace college /aip	Assessment police	2 week
2012	nogada	Training car guard	2 week
2022	Microsoft	Security policy information system,azure defender	2week
2023	Isc/sisco	Security information talk brite	month
2024	Met police uk	Recruitment training	month
2024	Scheineder	Security physical	
2025	Eaton	Security engineering	

D. QUALIFICATIONS

LIST ALL RELEVANT QUALIFICATIONS APPLICABLE TO THE POST YOU ARE APPLYING FOR (*HIGHEST SCHOOL AND TERTIARY QUALIFICATIONS COMPLETED):

YEAR	INSTITUTION	QUALIFICATION
2018	saqa	Award degre diploma
2020	Saqa /st peace college	Award diploma
2021	St peace college	Electrical certificate
2024	Alison	Diploma engineering
2024	scheinedr	Assessment expert
2025	Eaton	Assessment expert

E. DESCRIBE THE FUNCTIONS WHICH YOU PERFORM IN YOUR CURRENT POST

Senior engineering/ production engineering

F. PREVIOUS EXPERIENCE (from inception to date)

START DATE	END DATE	COMPANY (INSTITUTION)	REASON FOR LEAVING
2010	2014	Nogada	Court dismissal
2014	2017	Section one	Leave sick

NAME: nogada sa

ADDRESS OF COMPANY:

Eden val

EMAIL:info@nogada sa .co.za

POSTAL CODE

TEL. HOME				
TEL. WORK				
CELL.				

H. CERTIFICATE

1. I hereby apply for an appointment to a post in the South African Police Service. I am aware of the fact that there are limited posts and that no promises were made to me about an appointment in the South African Police Service.	
2. I am aware of the fact that:	
2.1	The National Commissioner is under no obligation to fill an advertised post;
2.2	I shall have to submit myself at my own expense and risk to any medical or other tests which are an inherent requirement for the post that may be required to finalize my application for appointment;
2.3	I have to provide full particulars concerning obligations to employers and debts if my application receives further consideration;
2.4	If my application does not meet the requirements stipulated in National Instruction 6 of 2005 as well as the advertisement, my application will be rejected;

2.5	If I am short listed I will be be subjected to a vetting process. I also agree to submit a set of fingerprints to the secretary of the selection committee for verification / vetting against the National Criminal Record Database as well as the National Register for Sex Offenders (NSRO);	
2.6	If I am found to be the final selected candidate for appointment in a post which forms part of certain identified categories, I will be subjected to a vetting process in terms of the prescripts of the Sexual Offences Act, 2007 (Act No 32 of 2007) and the Children's Act, 2005 (Act No 38 of 2005). If my name appears on either one of the National Registers, will be disqualified from appointment to that post. If it appears after an applicant's appointment that his / her name appears in either of the indicated registers, his/her appointment may be reconsidered.	
2.7 If I am found to be the final selected candidate and that it is discovered that I failed to disclose any criminal or disciplinary or civil matter (pending / conviction / sanction) against me, my application may be rejected / my appointment may be reconsidered;		

2.8 If I am found to be the final selected candidate and that it is discovered that I failed to disclose that I am a respondent in an interim or final protection order in terms of the Domestic Violence Act, 1998 (Act No 116 of 1998) or Protection from Harassment Act, 2011 (Act No 17 of 2011), my application may be rejected / my appointment may be reconsidered;	
2.9 If at any stage it is discovered that I have disclosed false information or failed to disclose any information which may have affected my candidature my application / and or candidature may be rejected / my appointment may be reconsidered; and	
3	I certify that all the information supplied by me on this application form is in all respects true and correct.
Date: …28/05/2025……	

Place: ……jhb / ……	**SIGNATURE OF APPLICANT**

Column8	Column9	Column10	Column11	Column12	Column13	Column14	Column15	Column16	Column17

your interests!

niques that intertwine calculus for precise applications. Let's integrate advanced calculations relevant to these topics and explore the

ons, and integrate:

10 \, \text{s}:

t's refine the exploration further!

ment information systems, **incident collision scenarios**, **patrol methods**, **community policing**, **communication skills**, **operation**

or decision-making and resource allocation.

t’s refine the learning further!

provides significant tools for solving real-world challenges. Here's how calculus concepts can enhance the understanding of these to

(x, y), where xx and yy are spatial coordinates.

. \]

mpact.

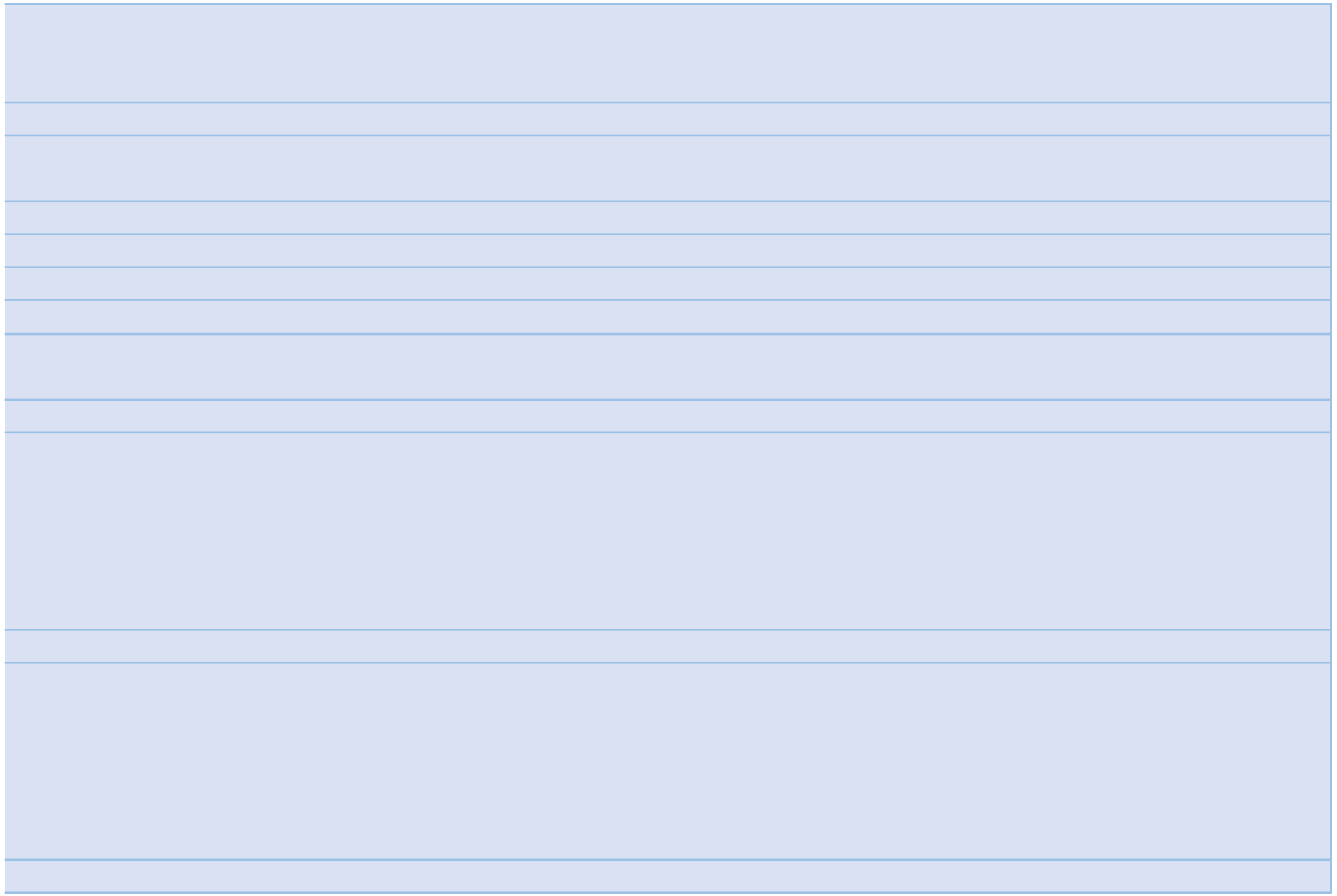
).

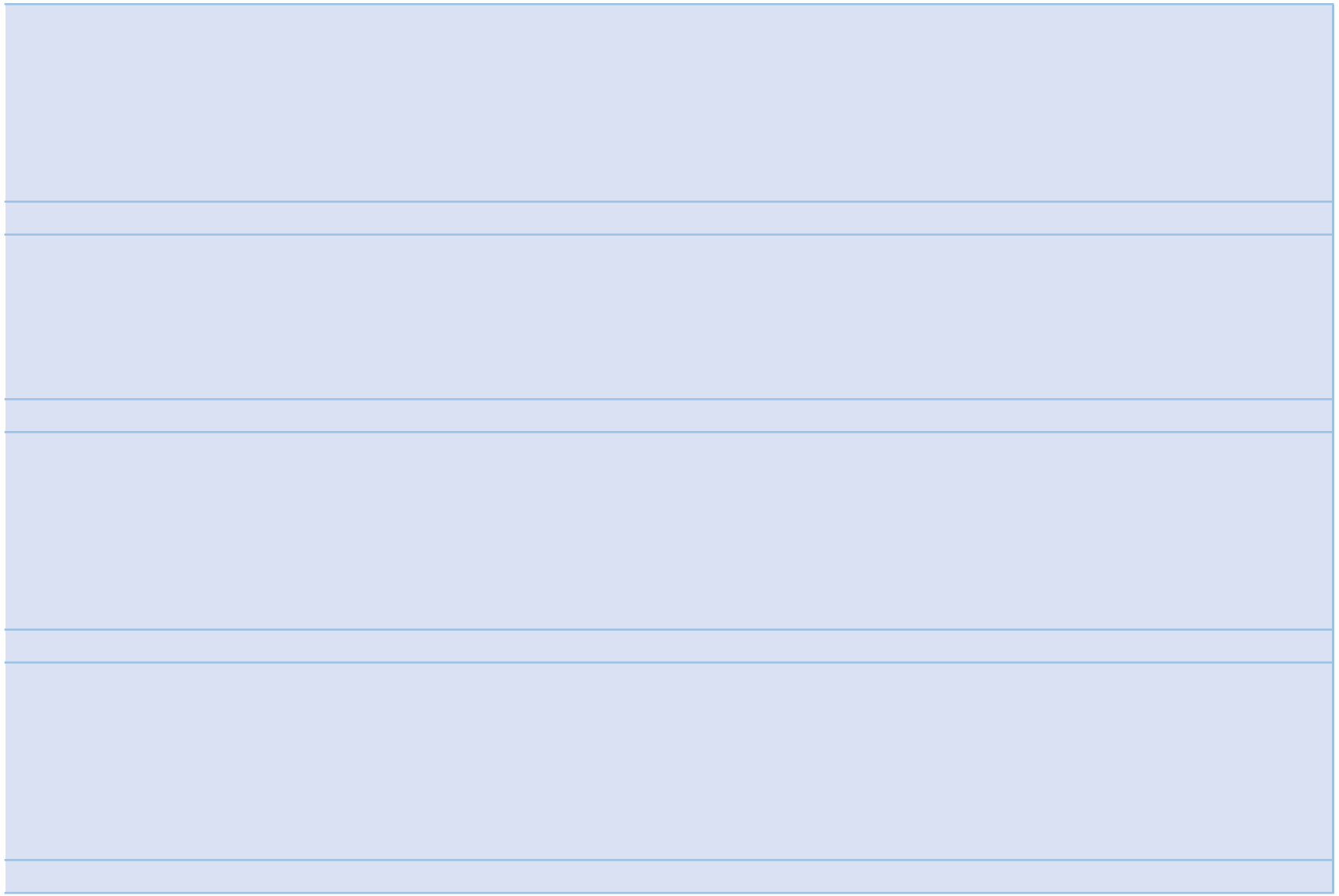
ter 10 days:

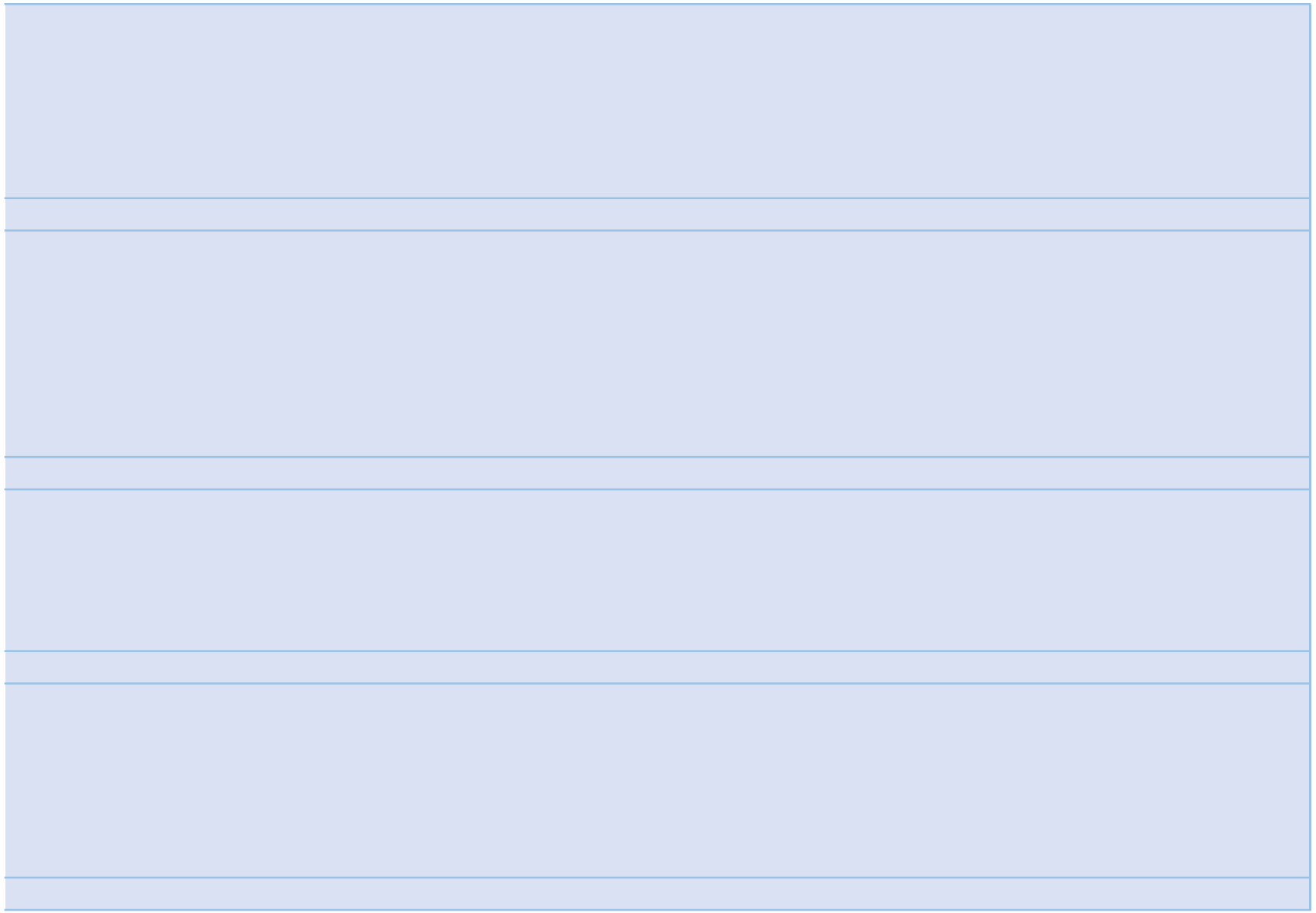
nalyzing forensic evidence. Let me know if you'd like further elaboration or custom examples tailored to your field of interest!

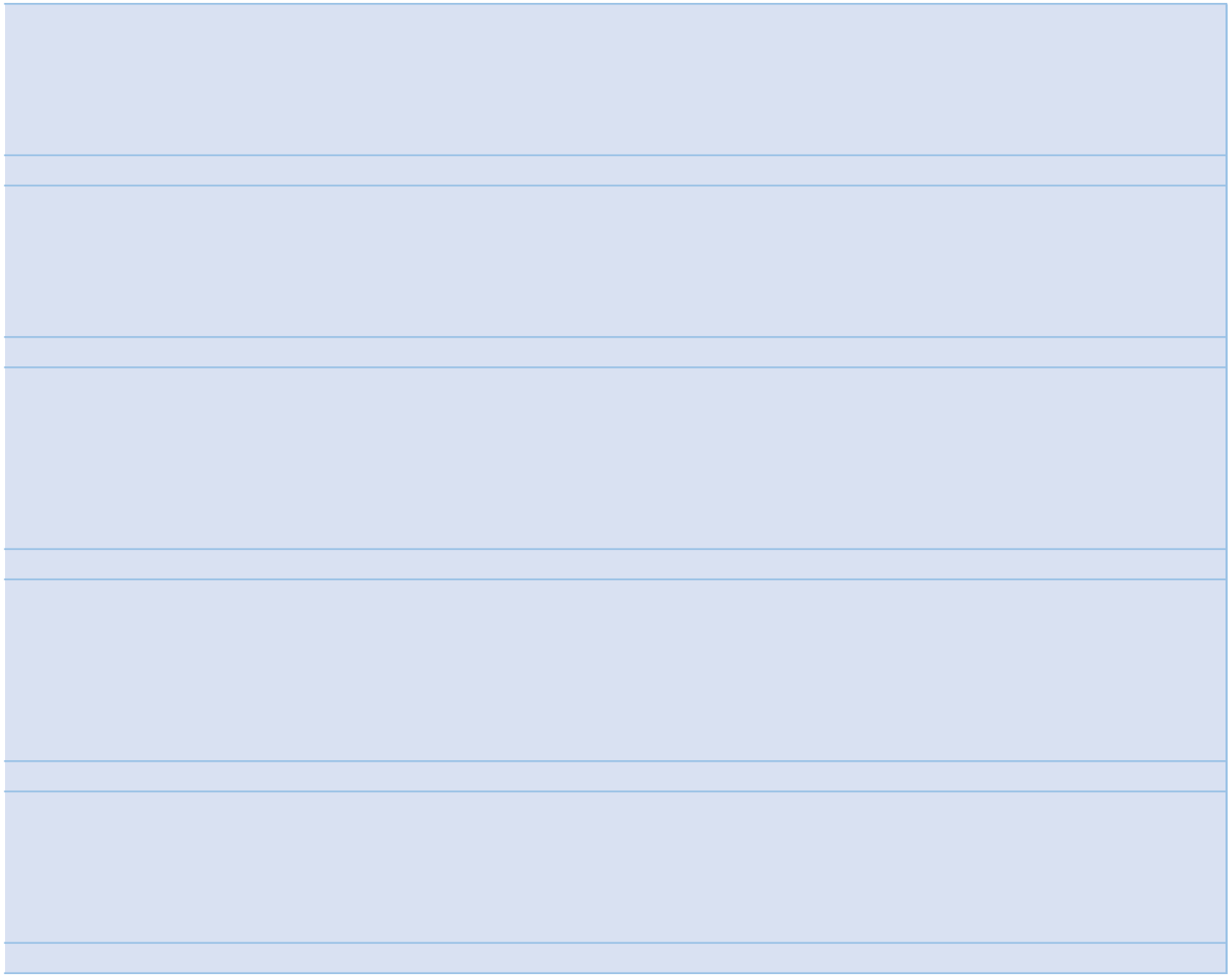
ional and advanced skills for the digital age. Here's a detailed breakdown of these fields, their purpose, experimental applications, an

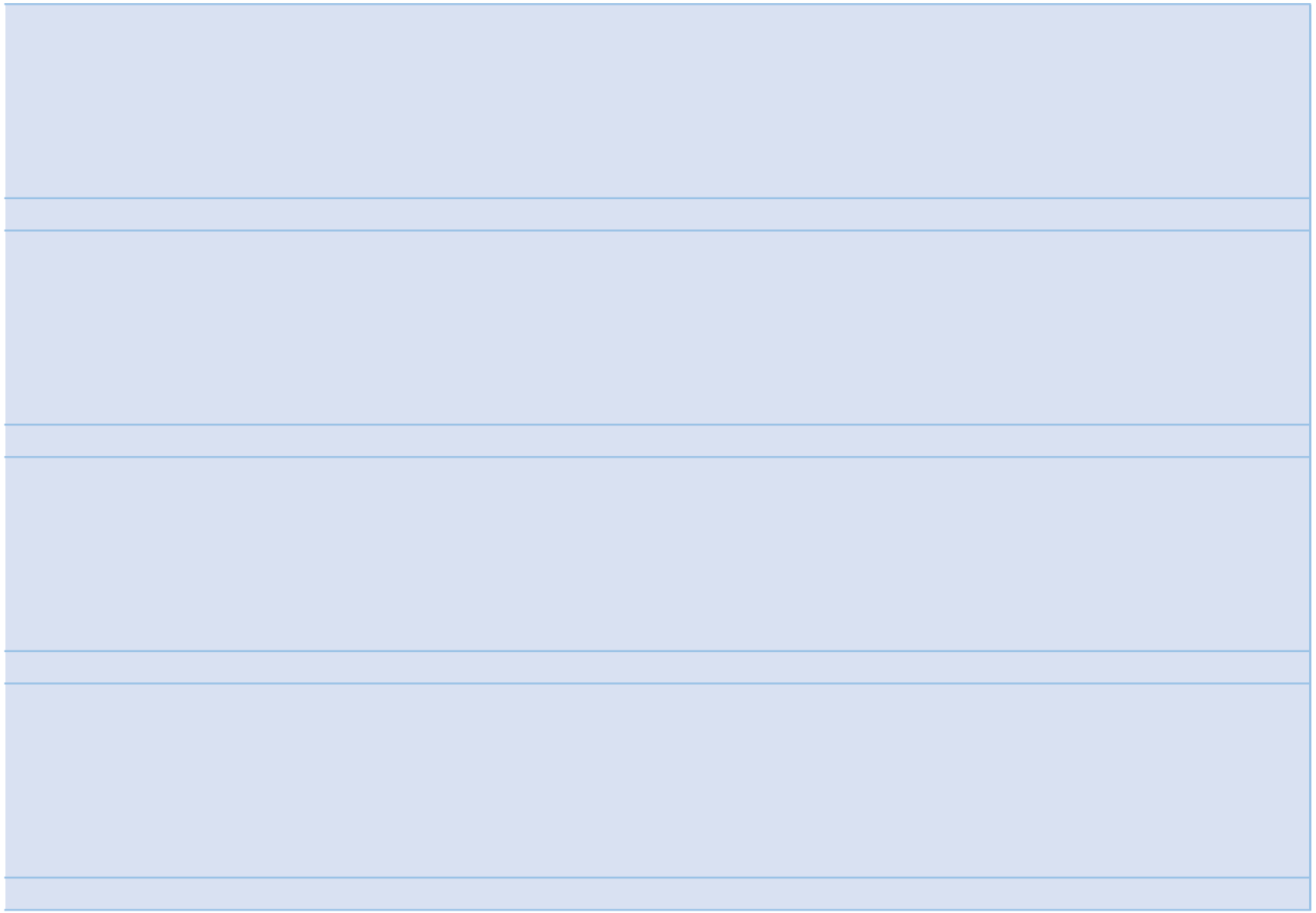
Column6	Column7	Column8	Column9	Column10	Column11	Column12	Column13	Column14	Column15

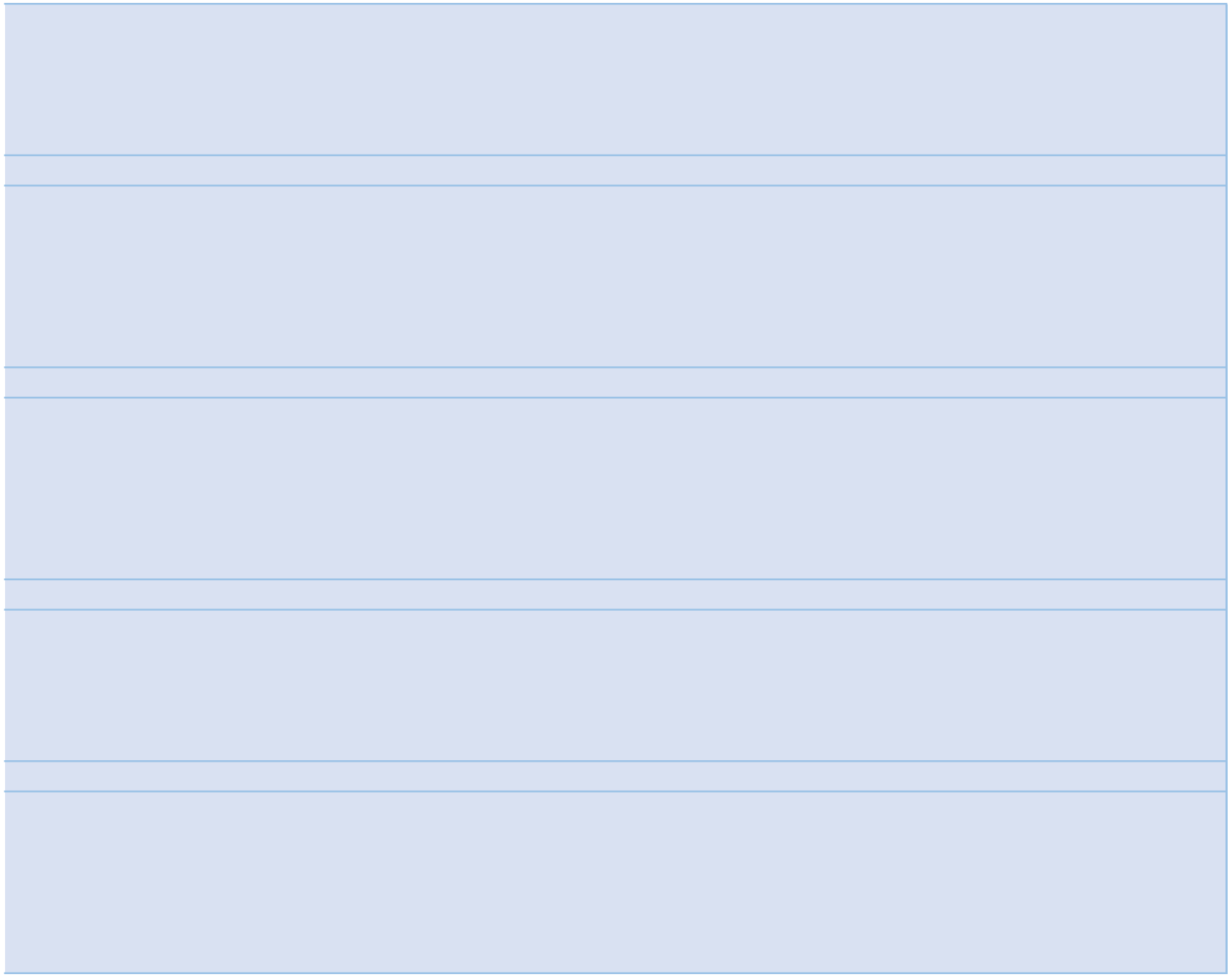


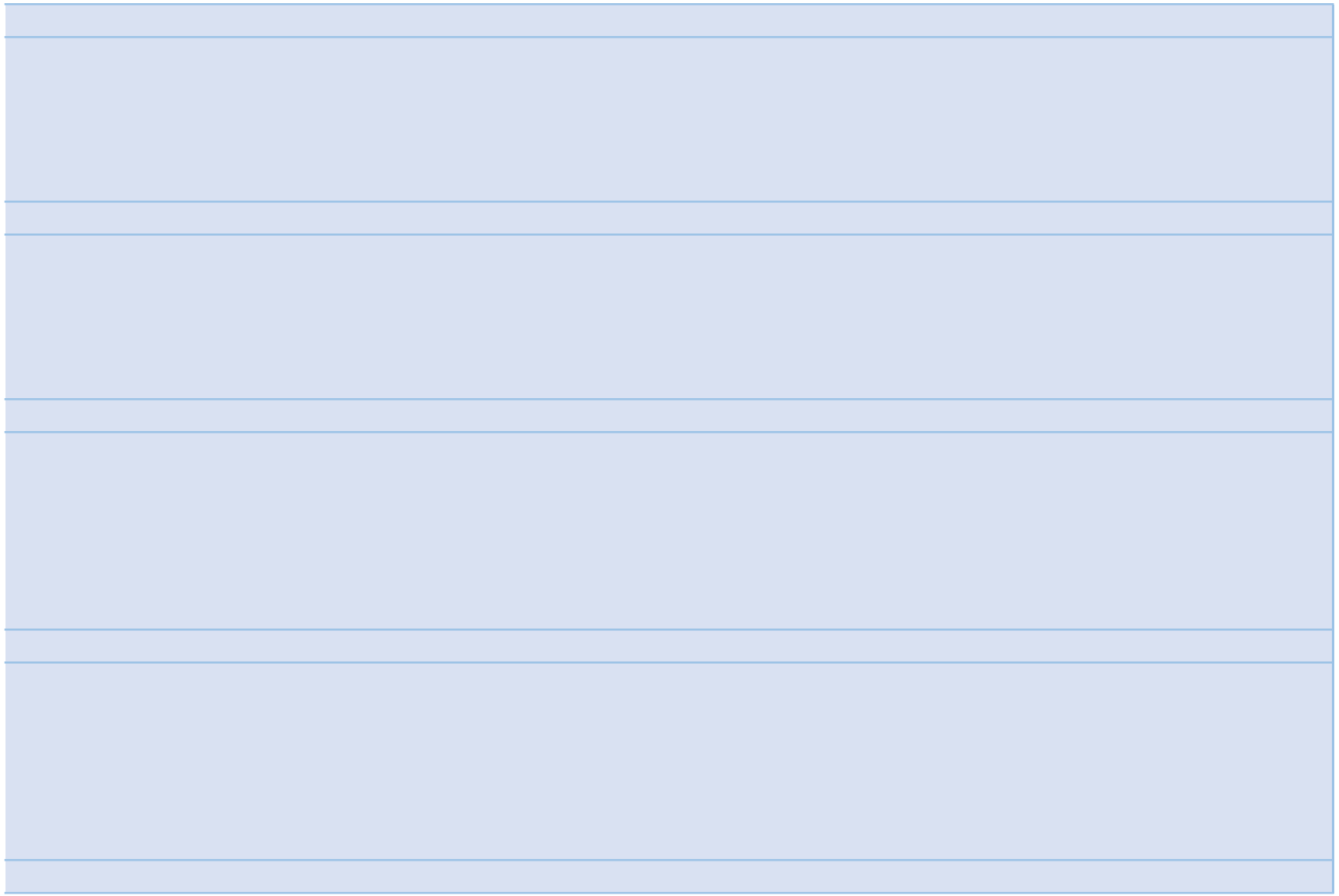


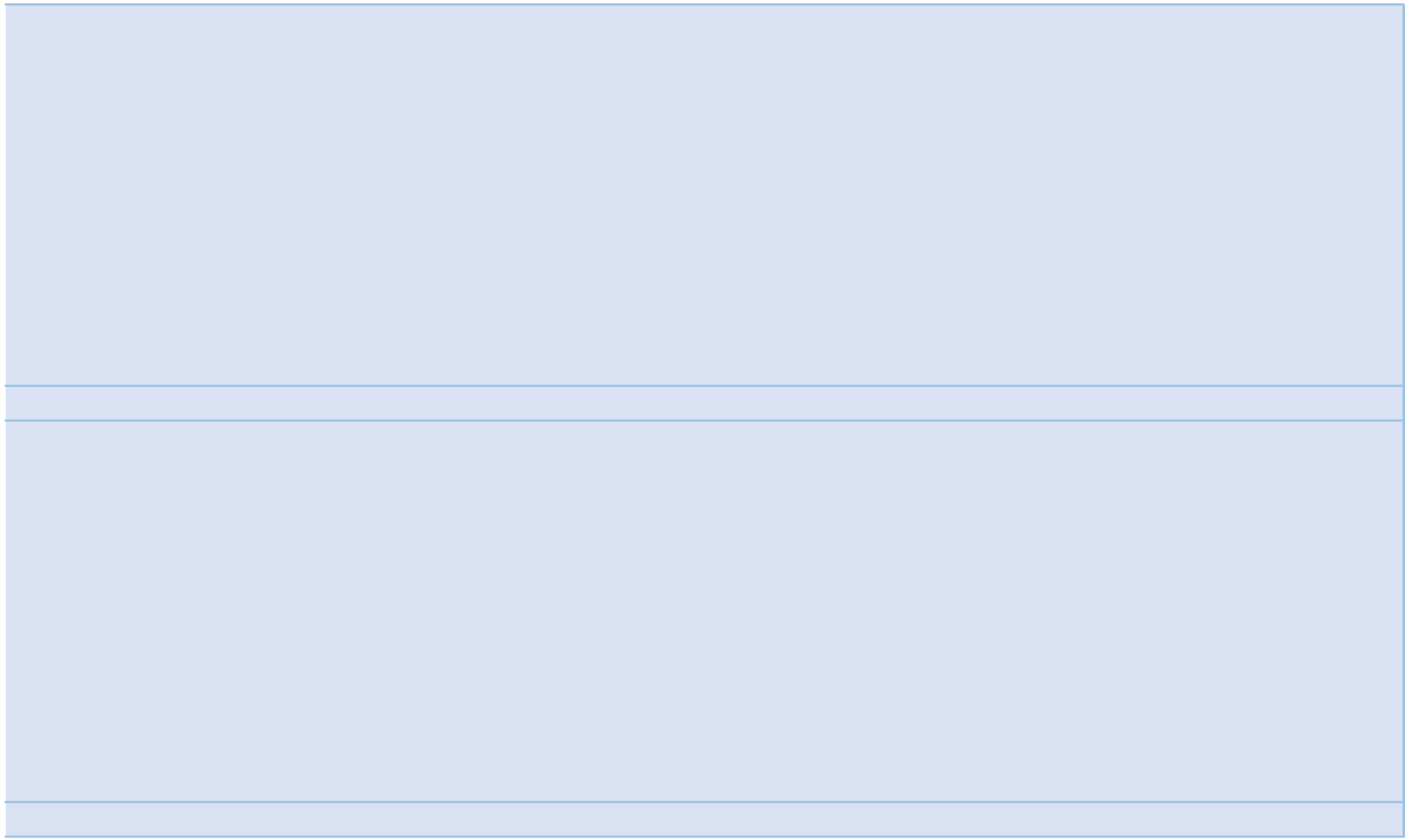


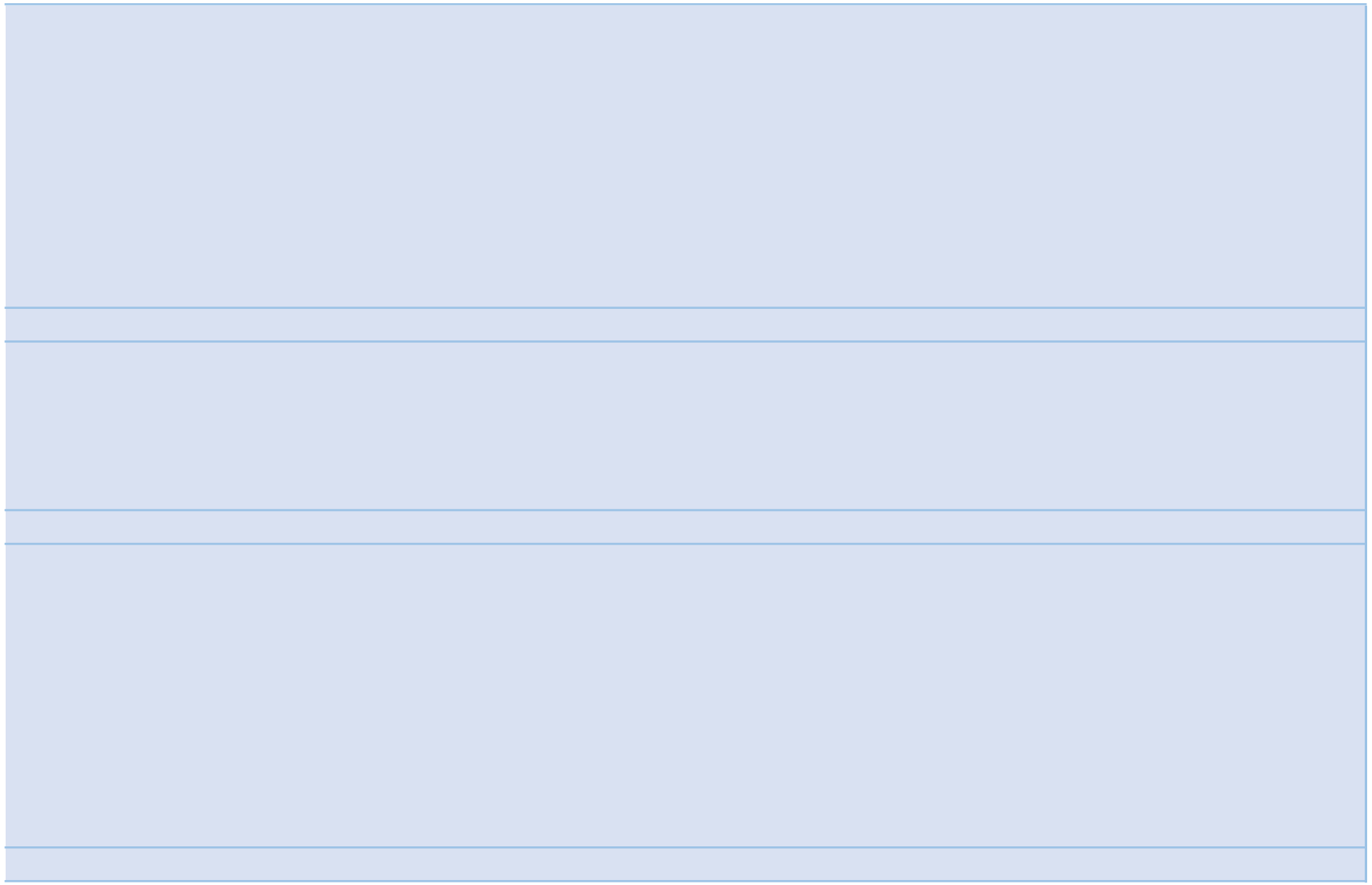


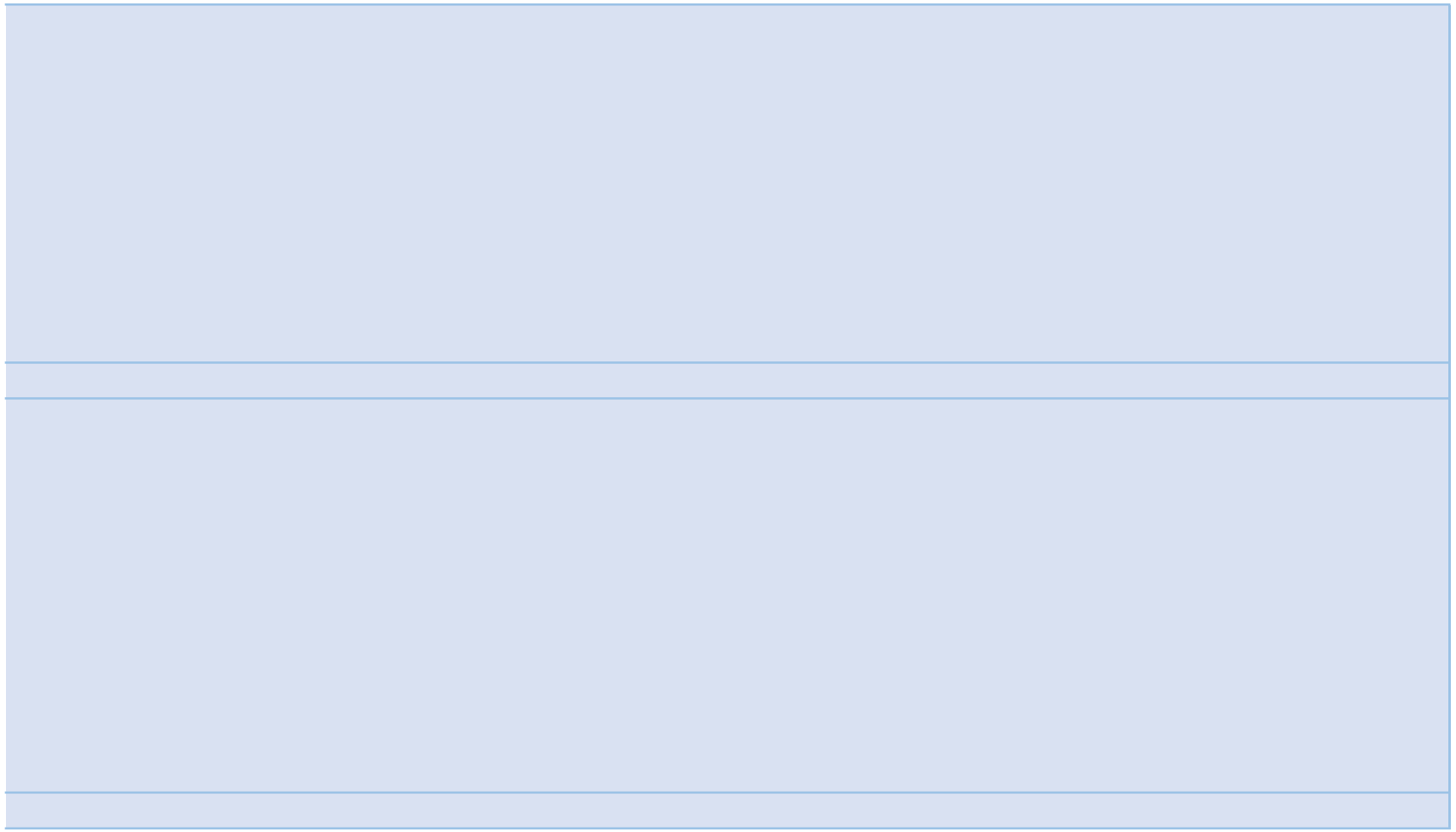


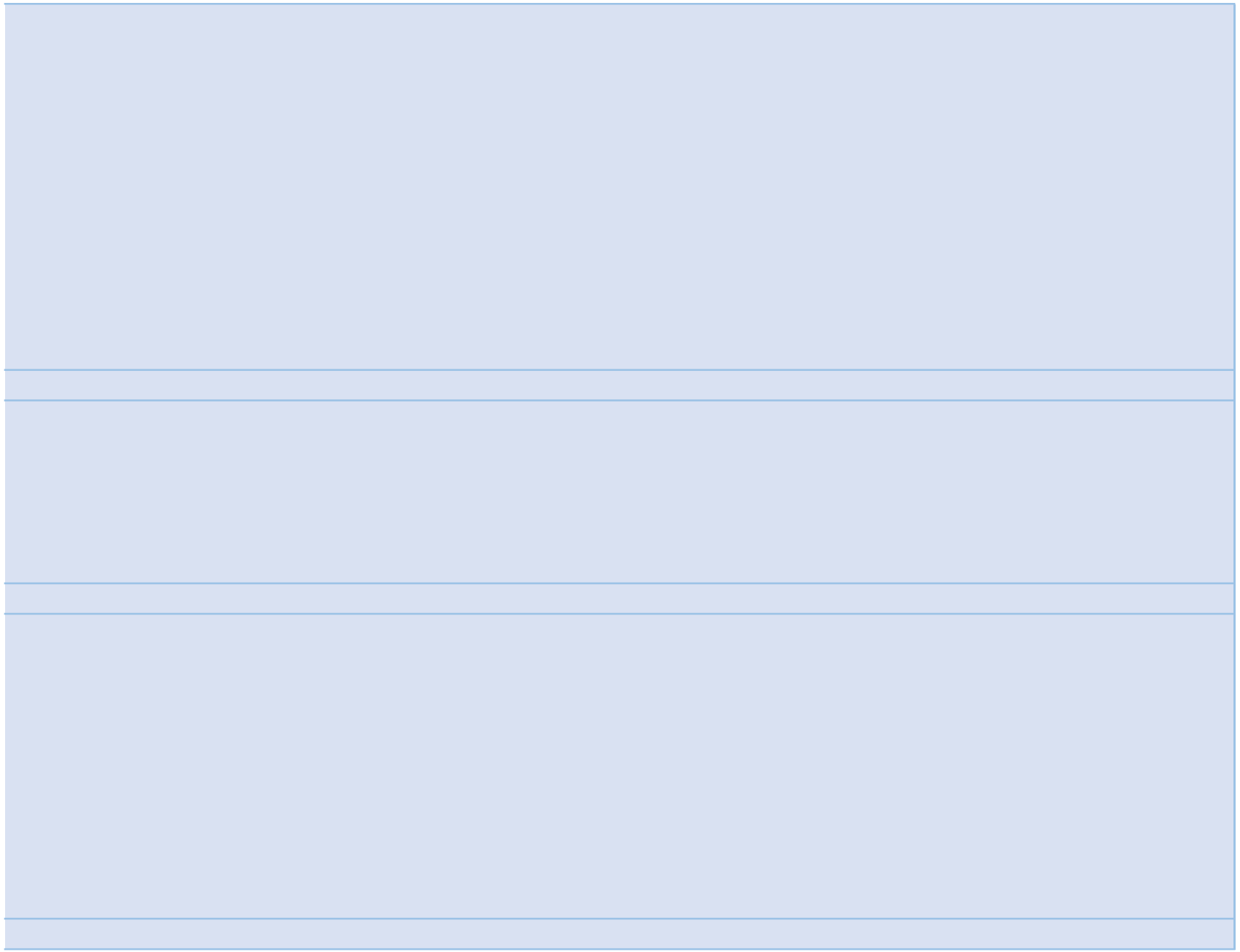


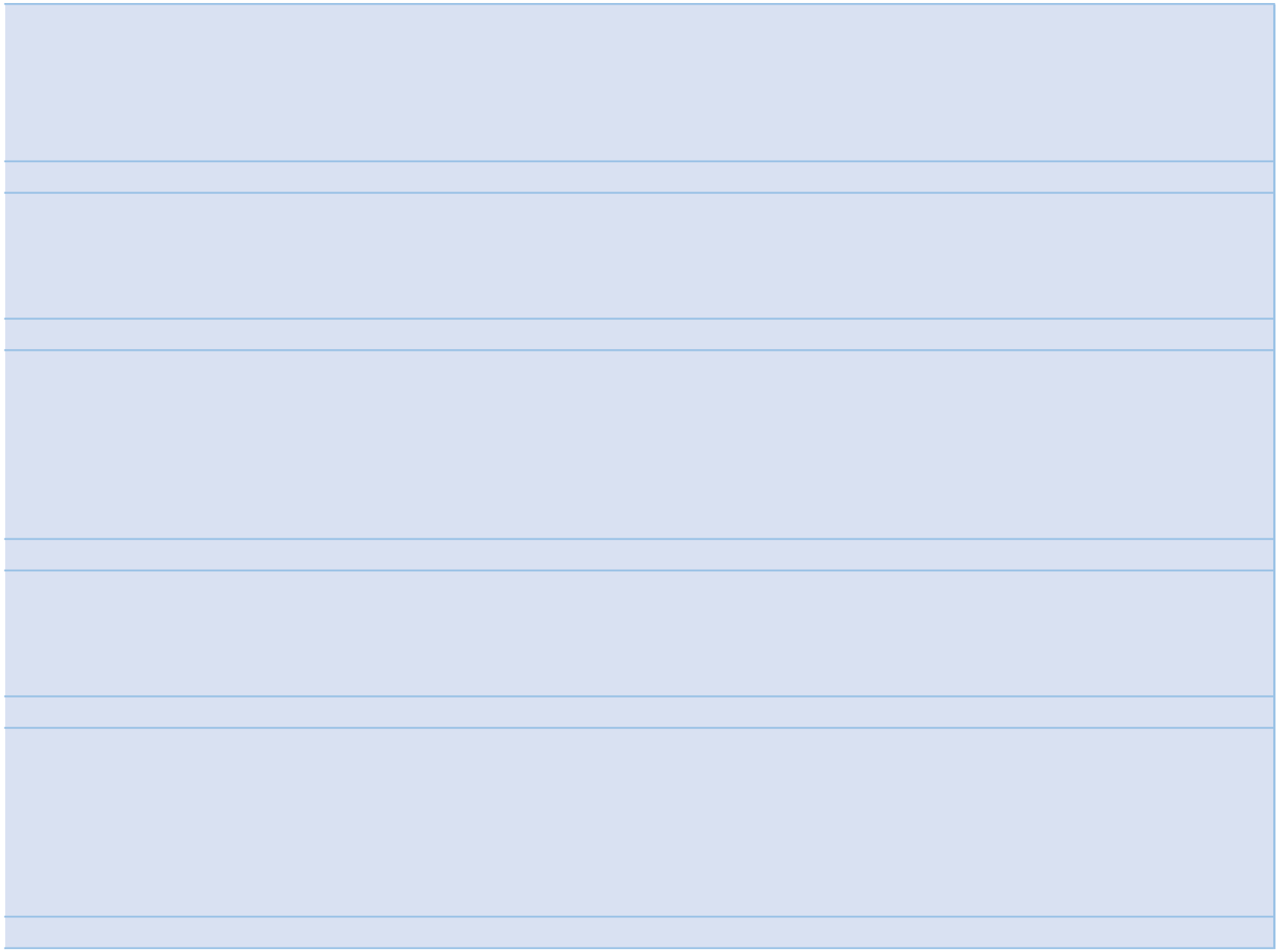


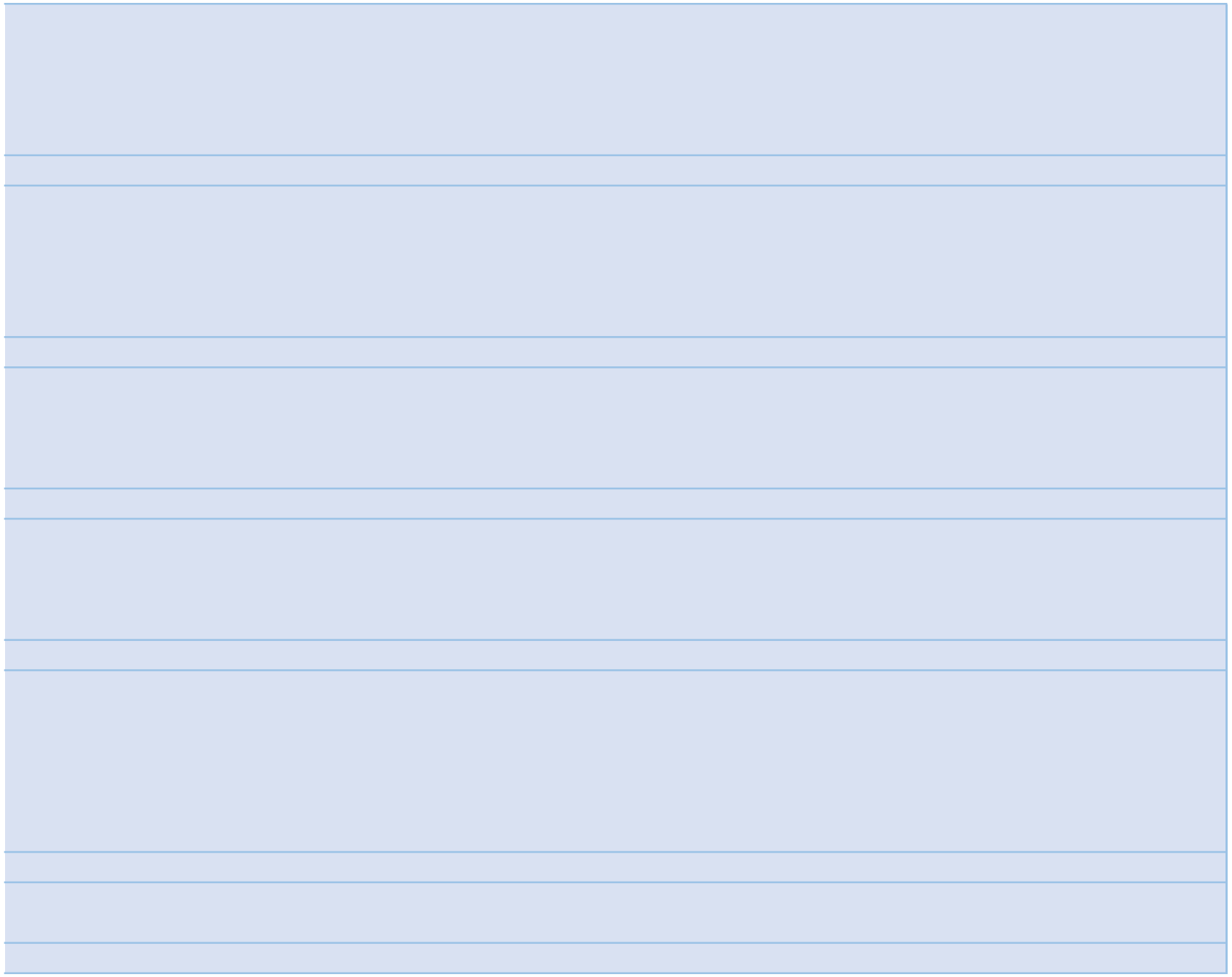


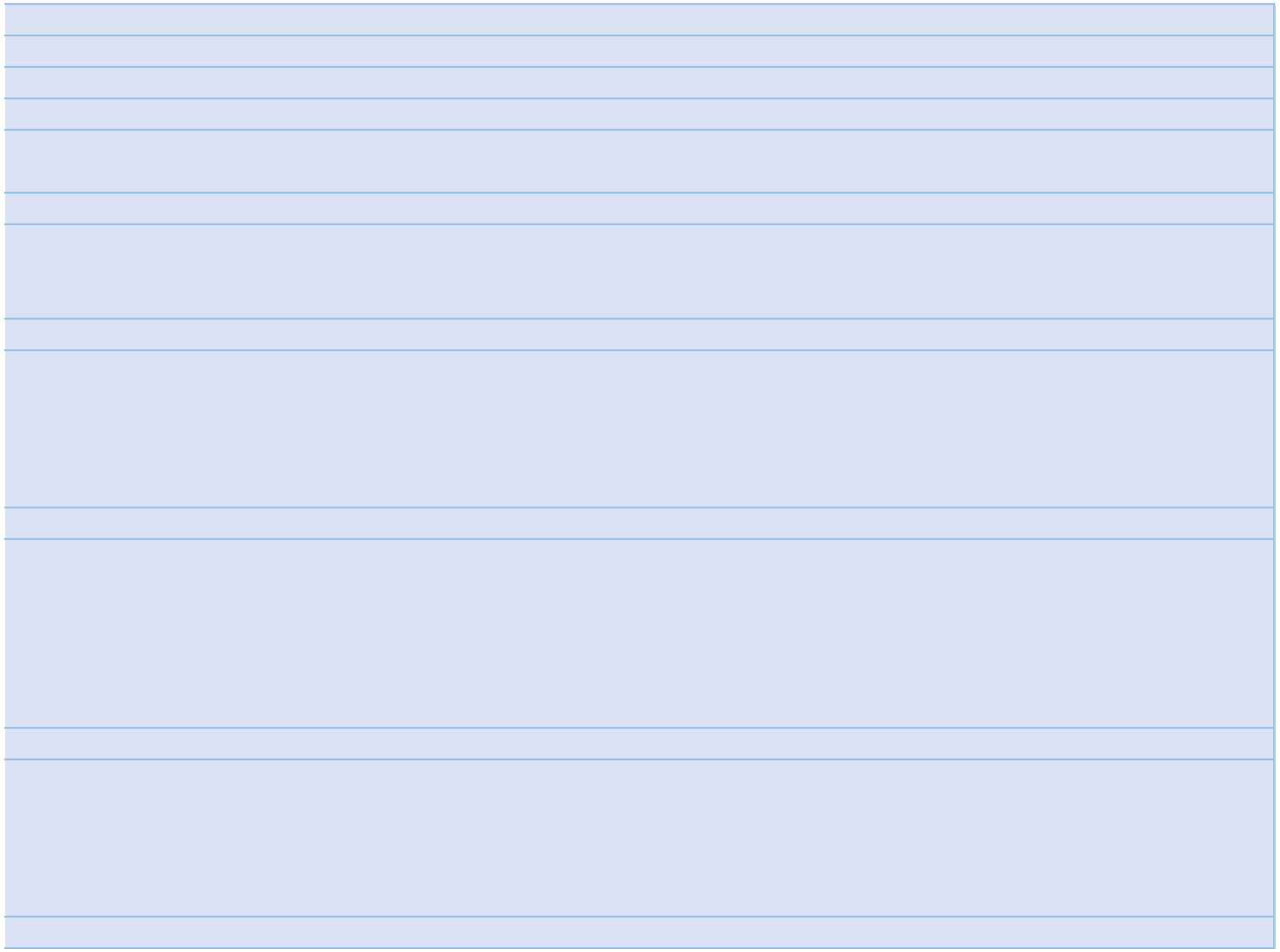


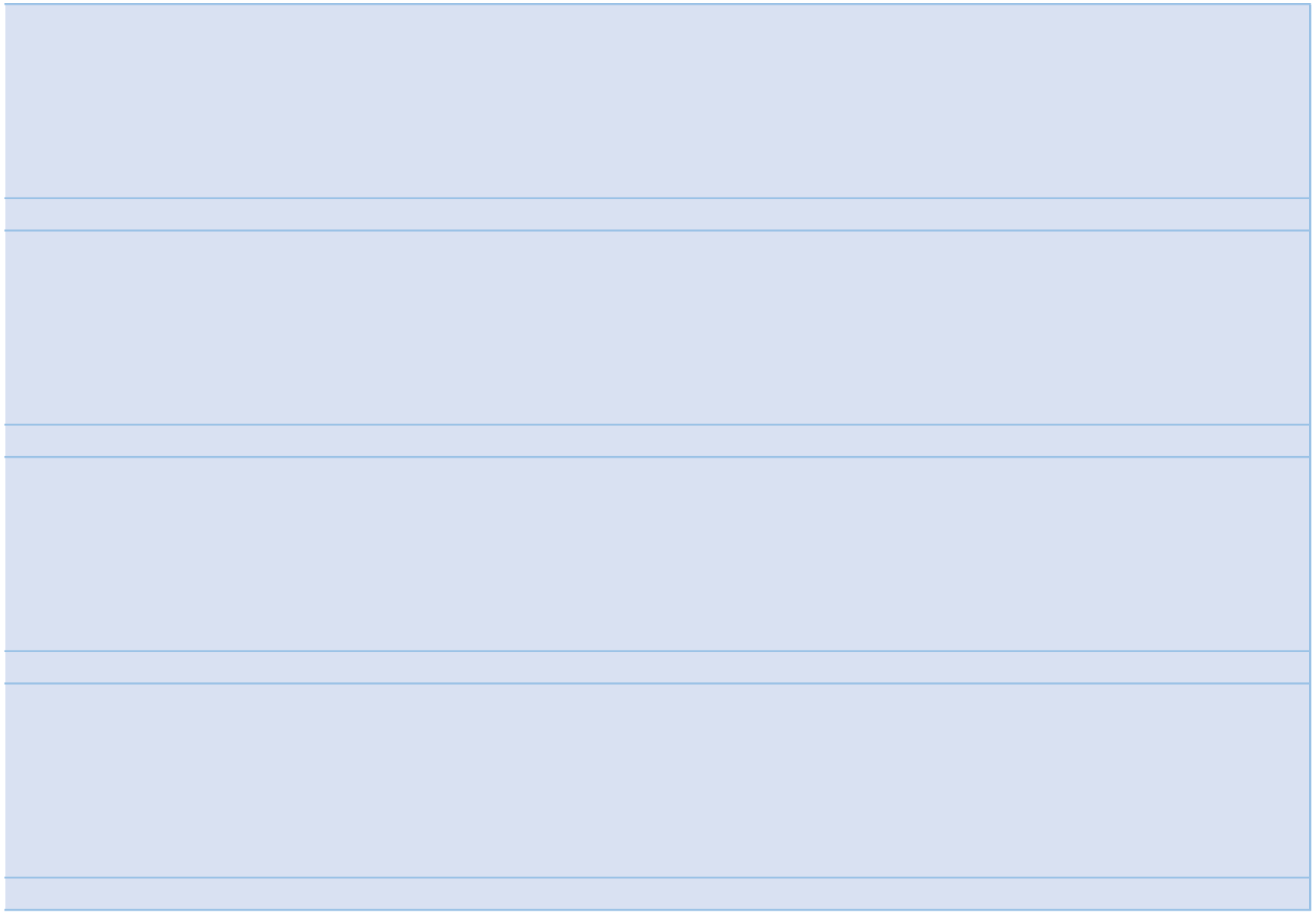


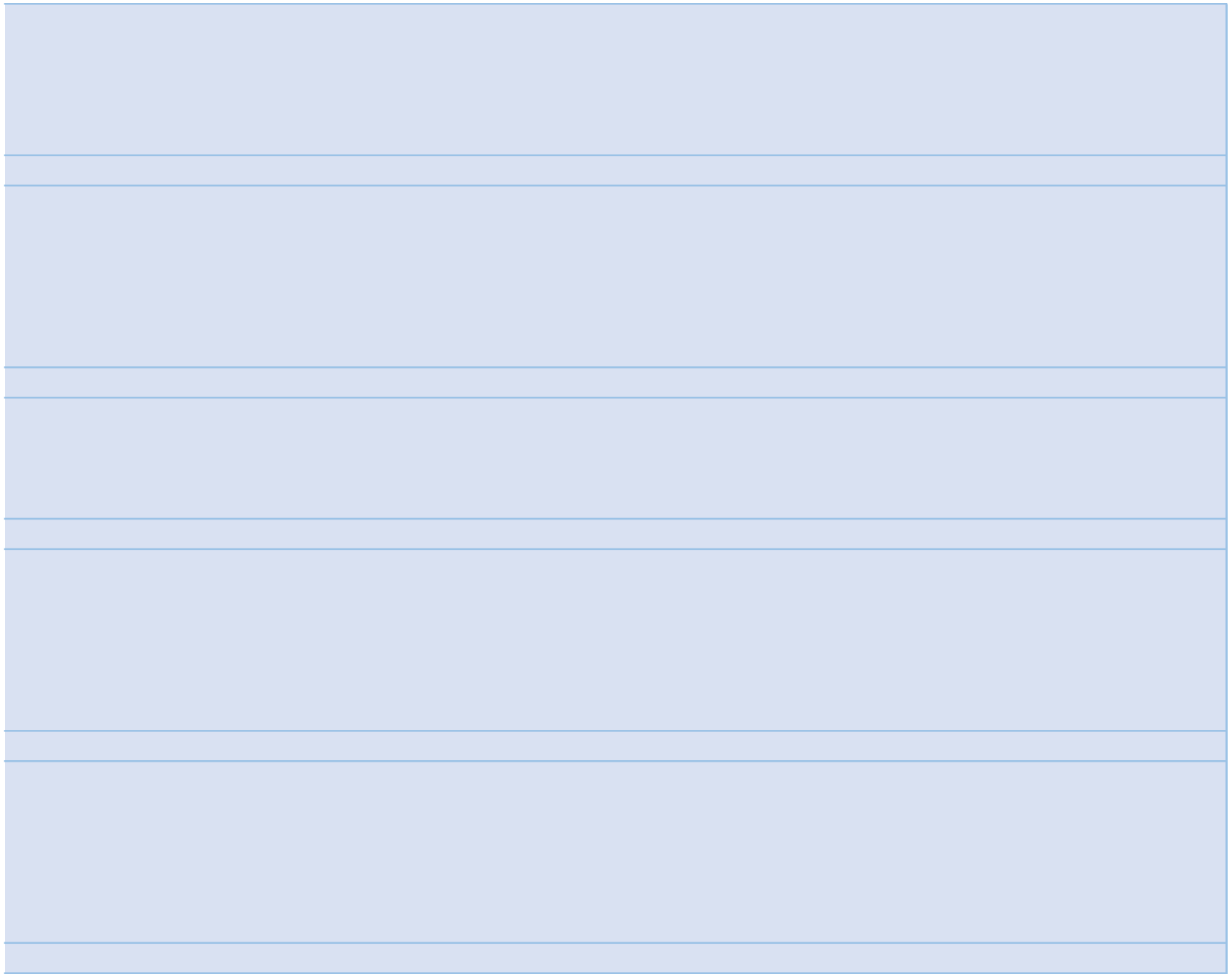


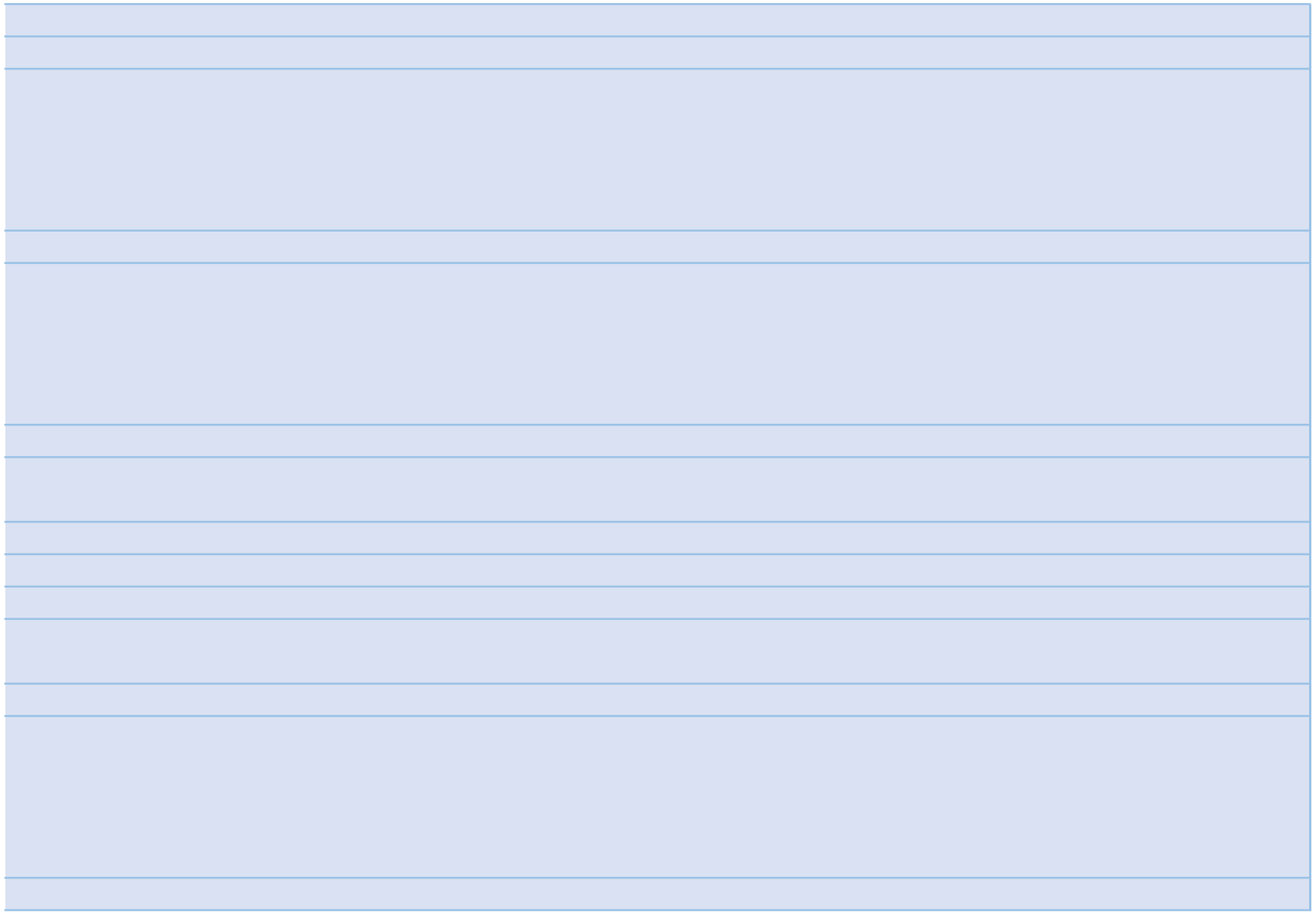


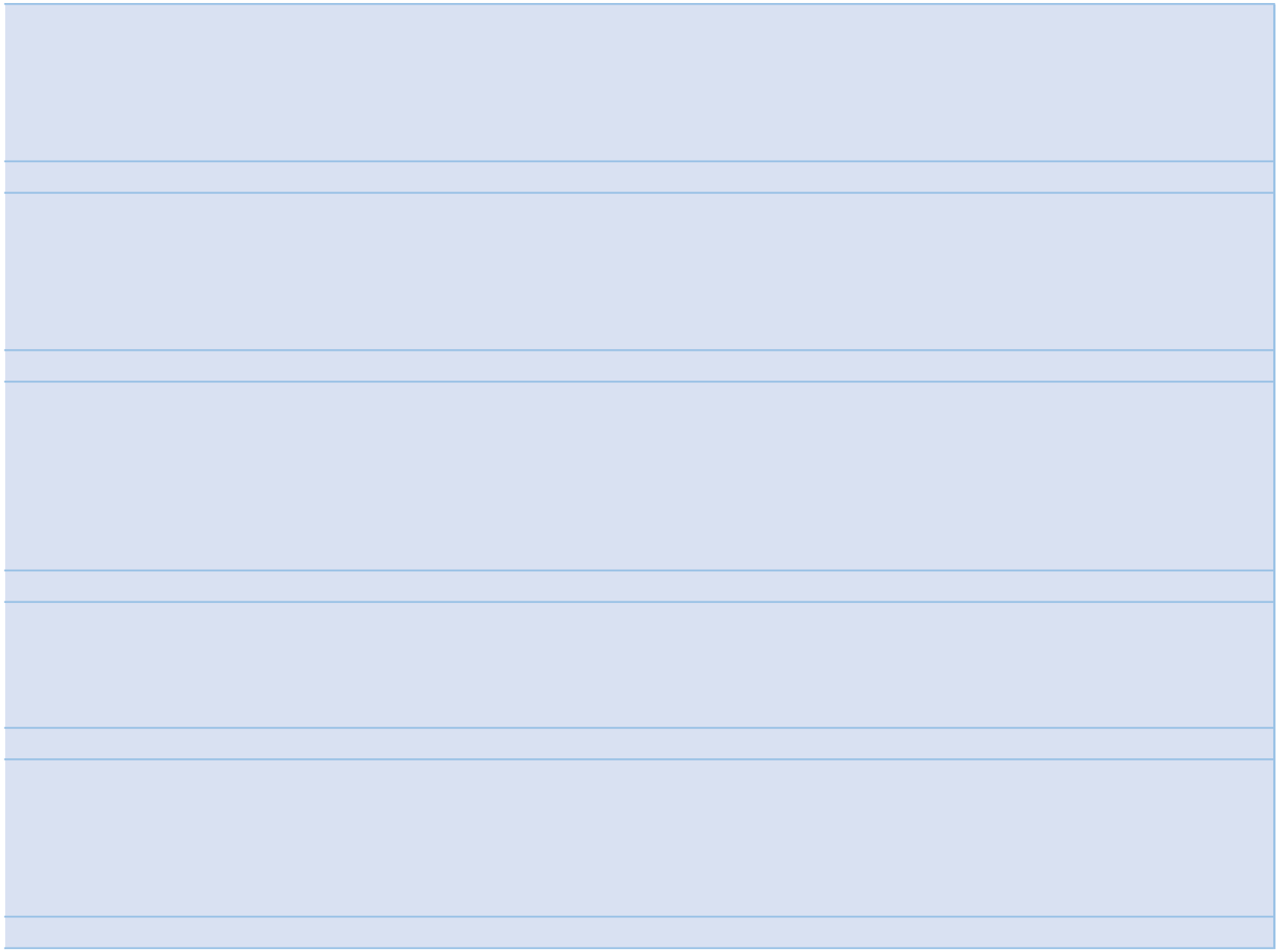


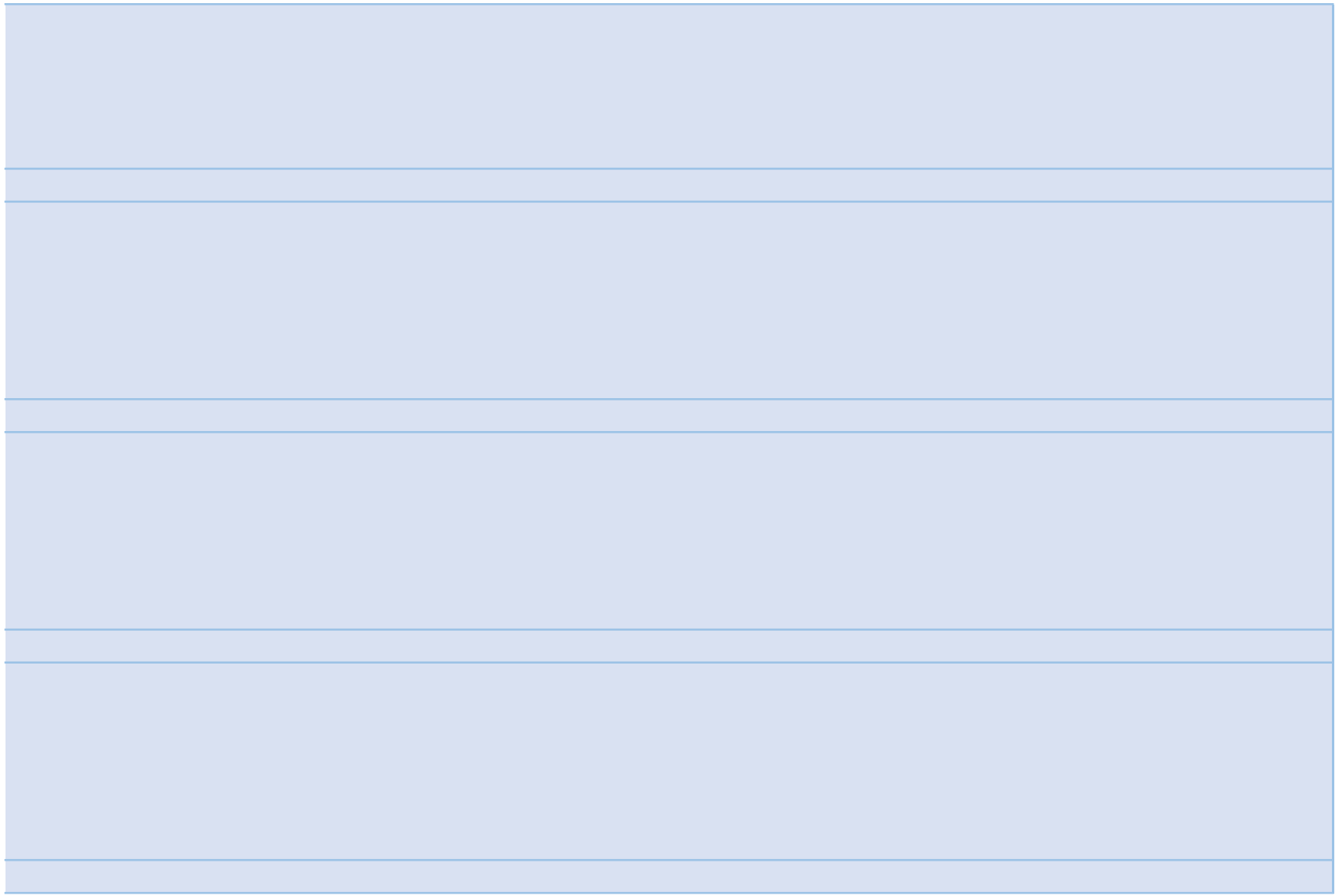


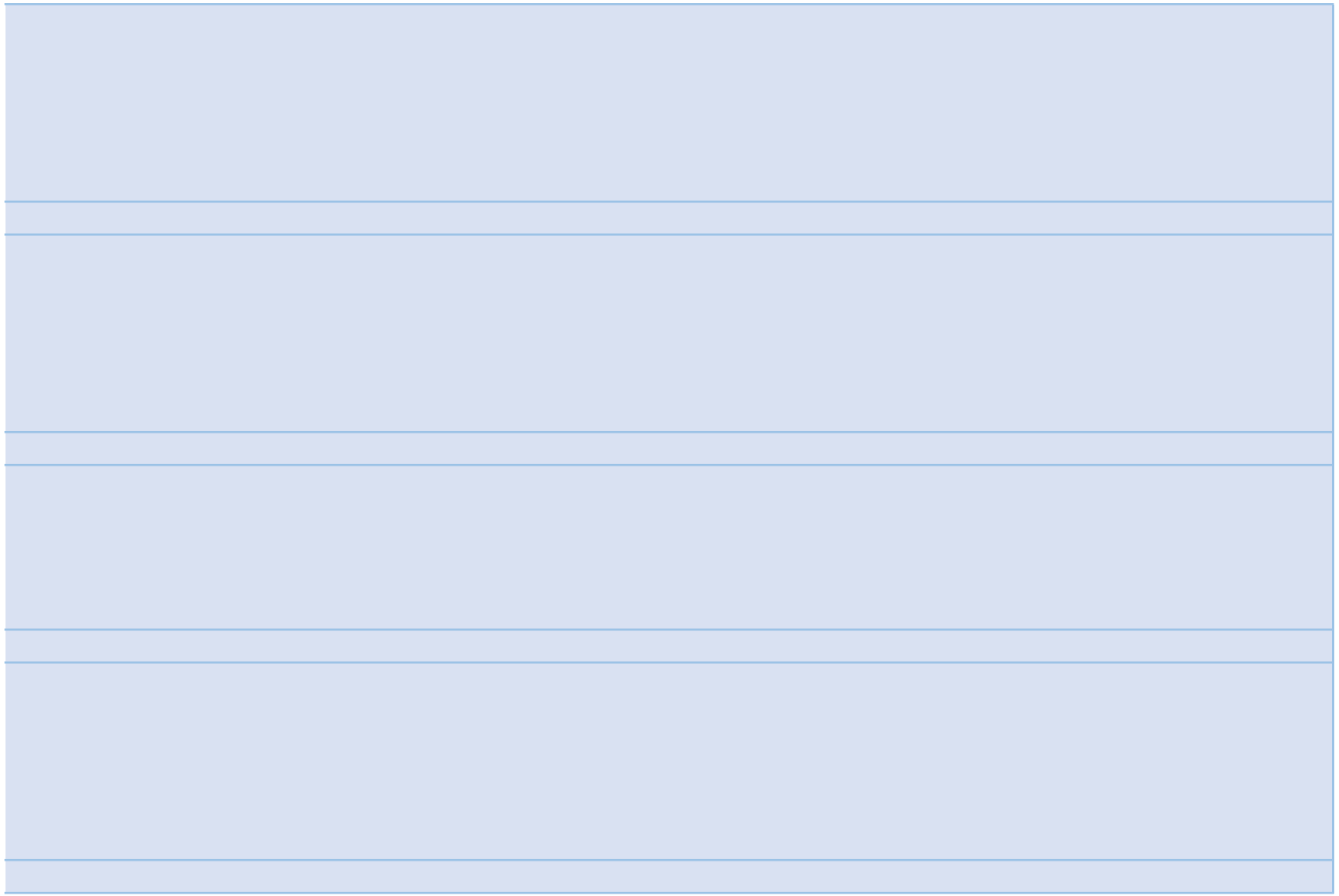


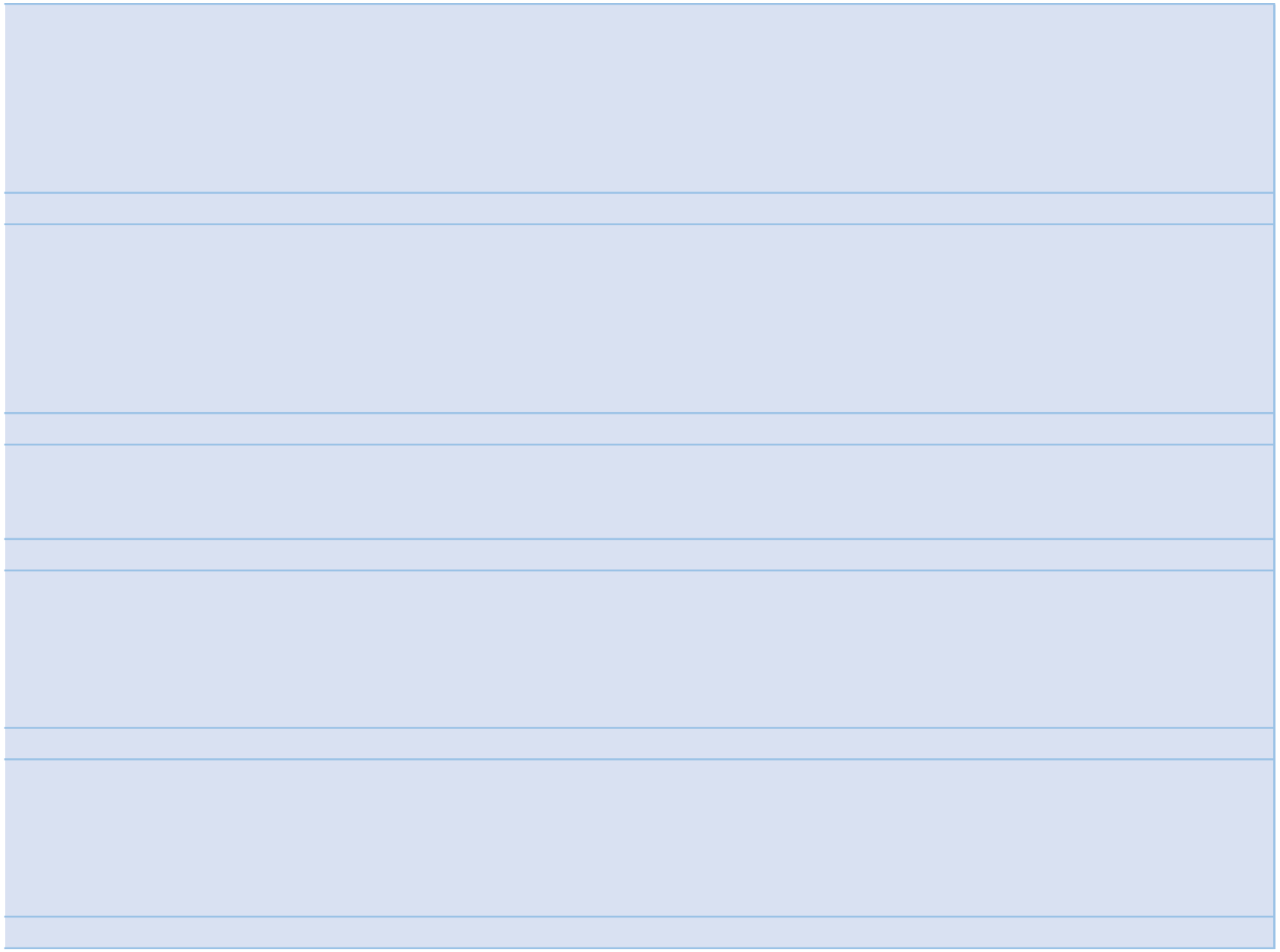


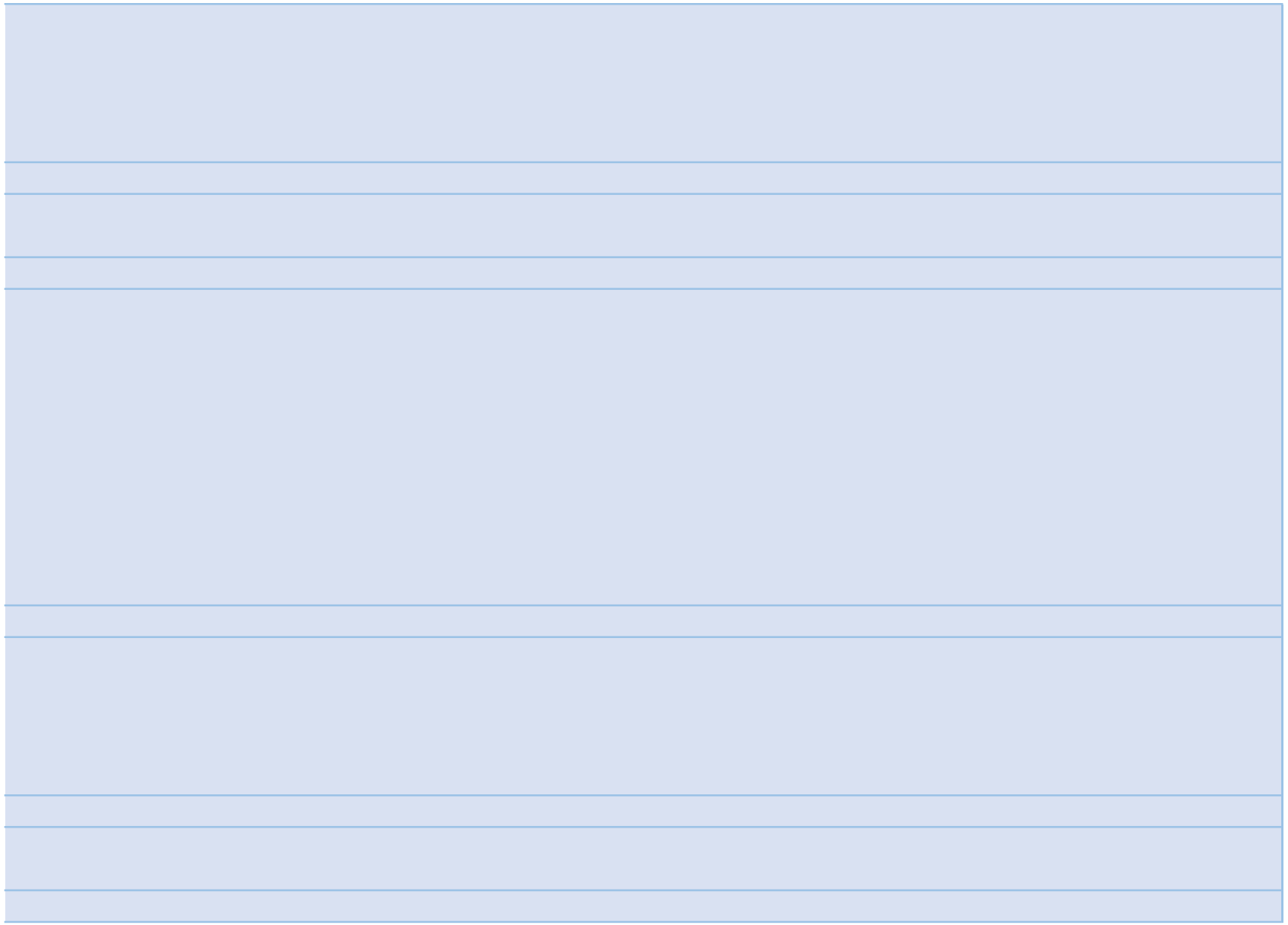


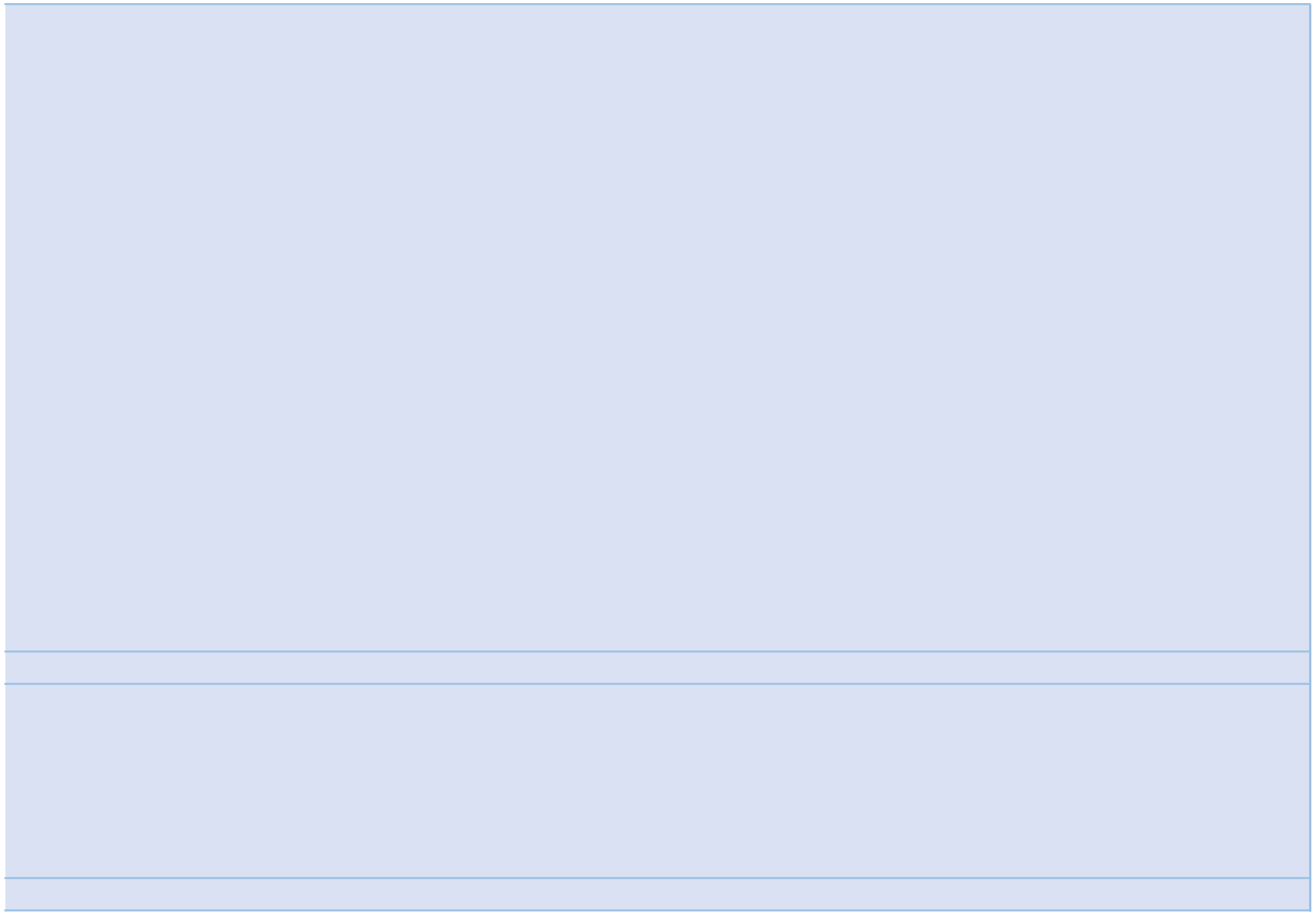


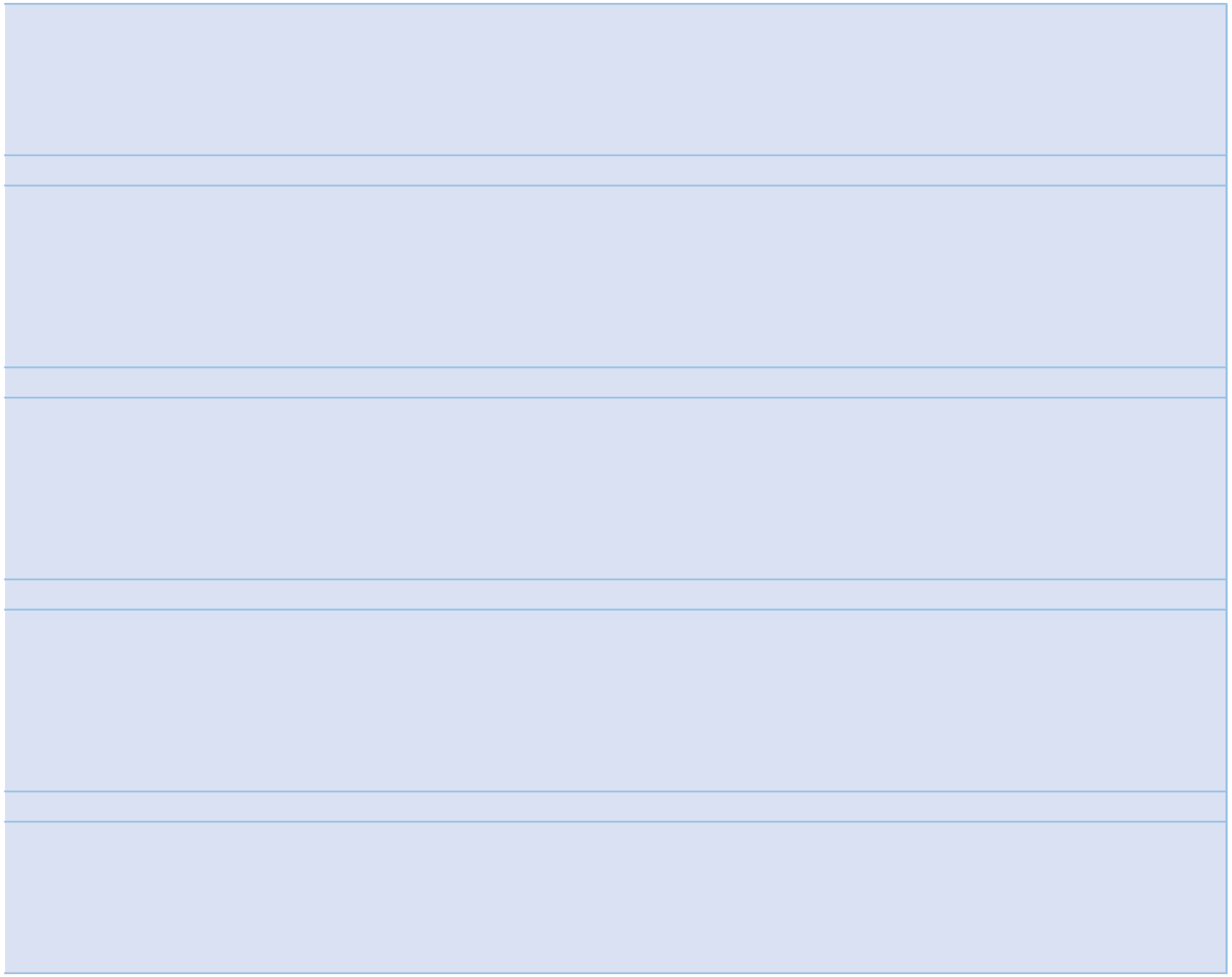


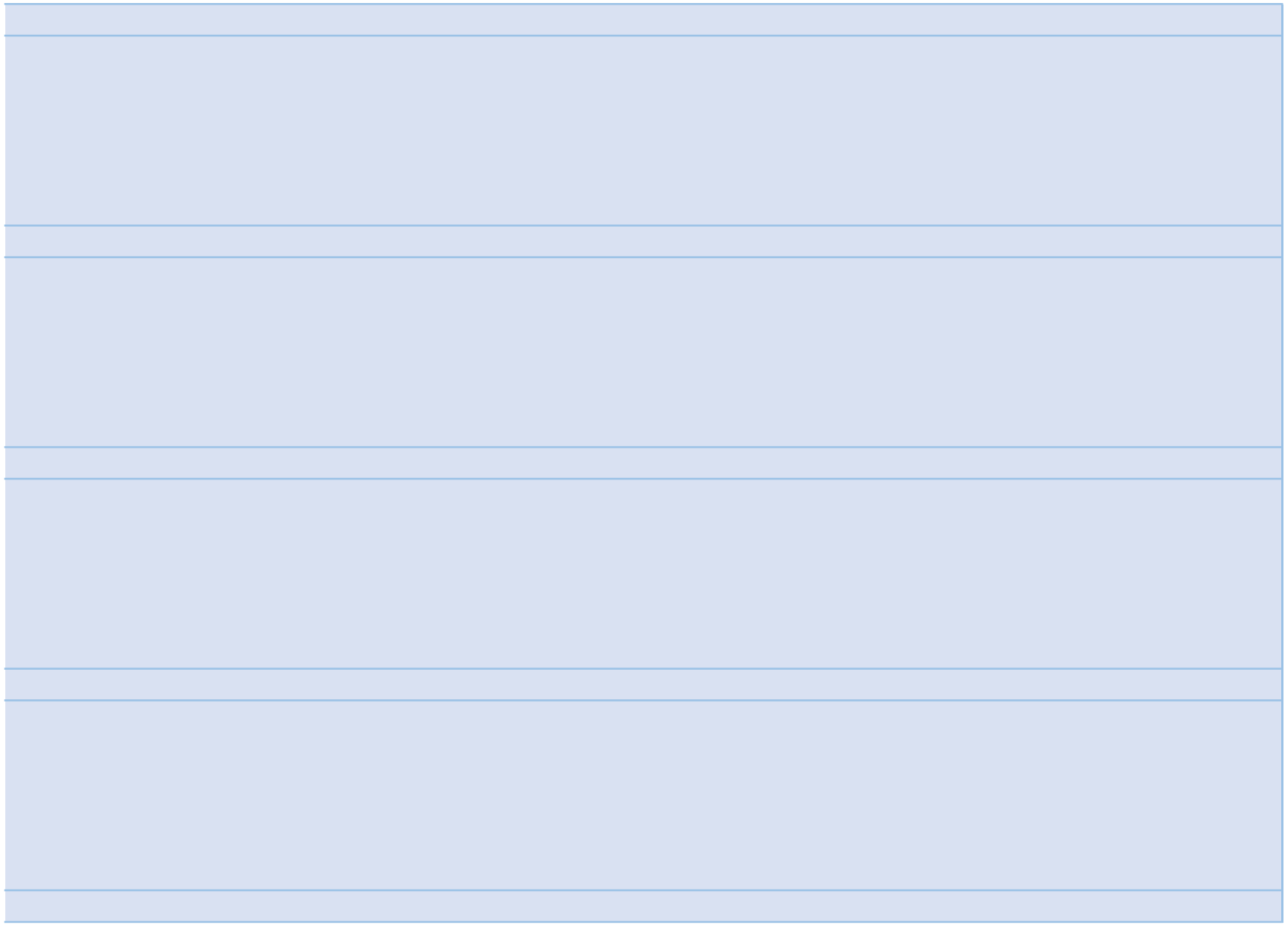


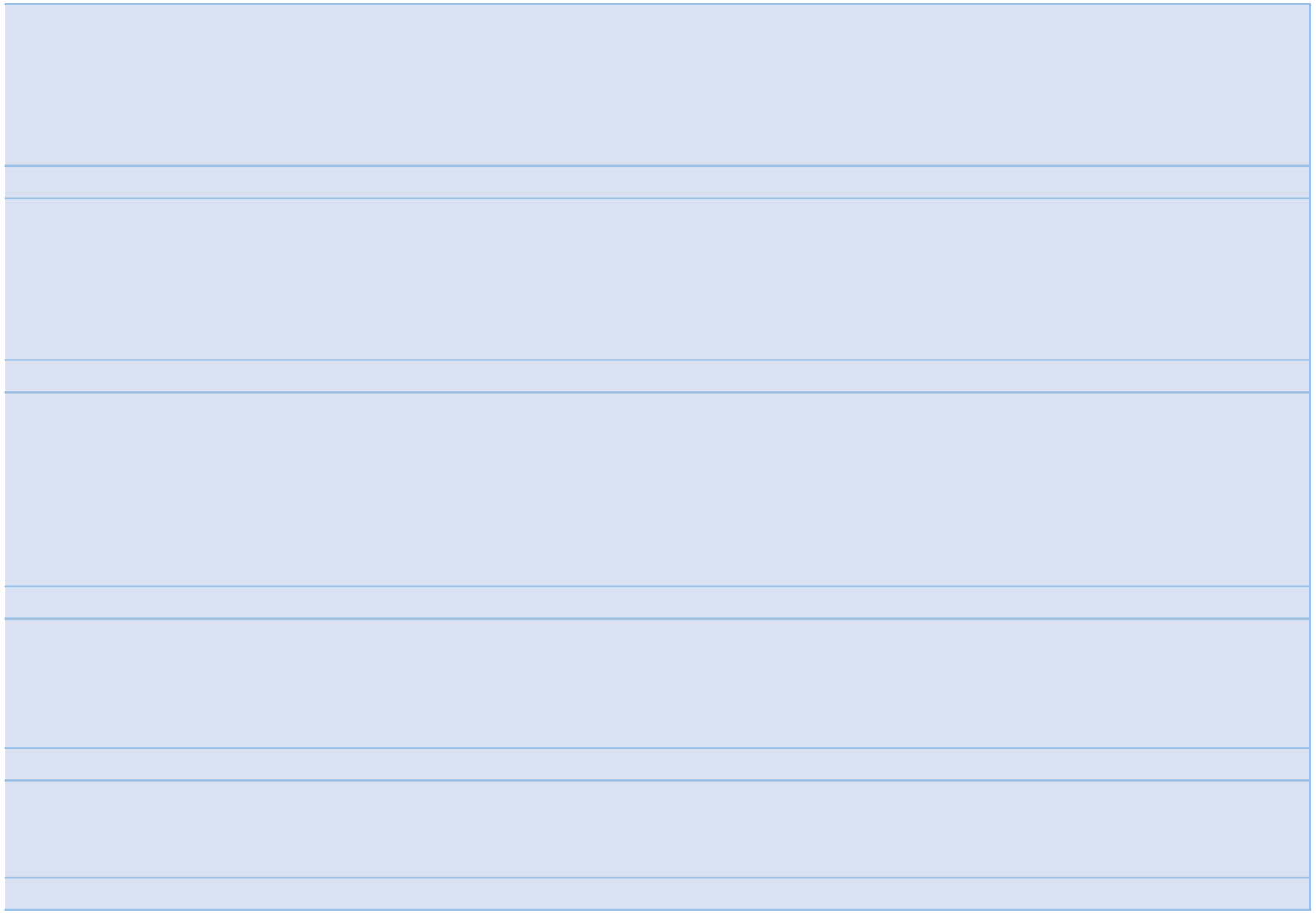


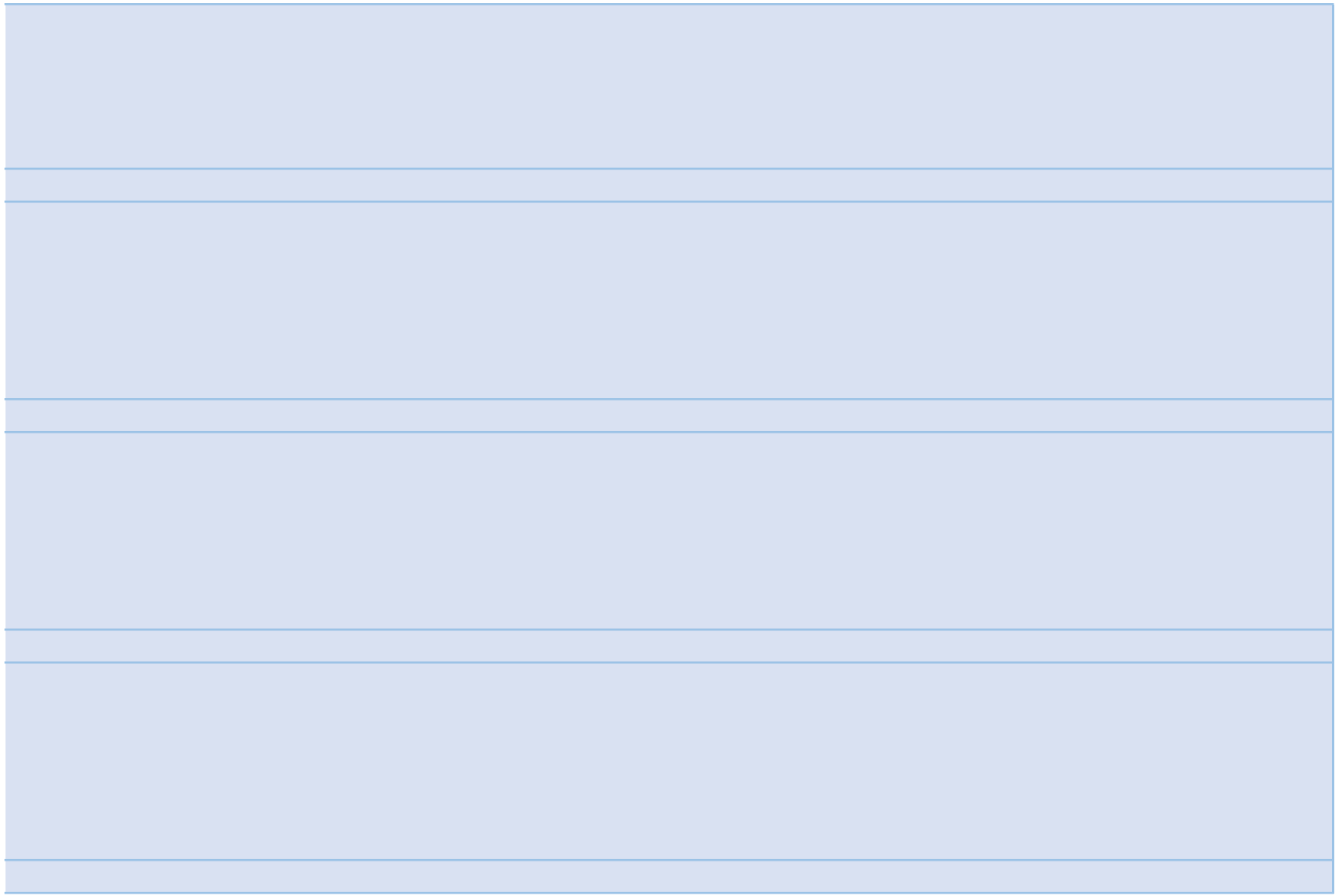


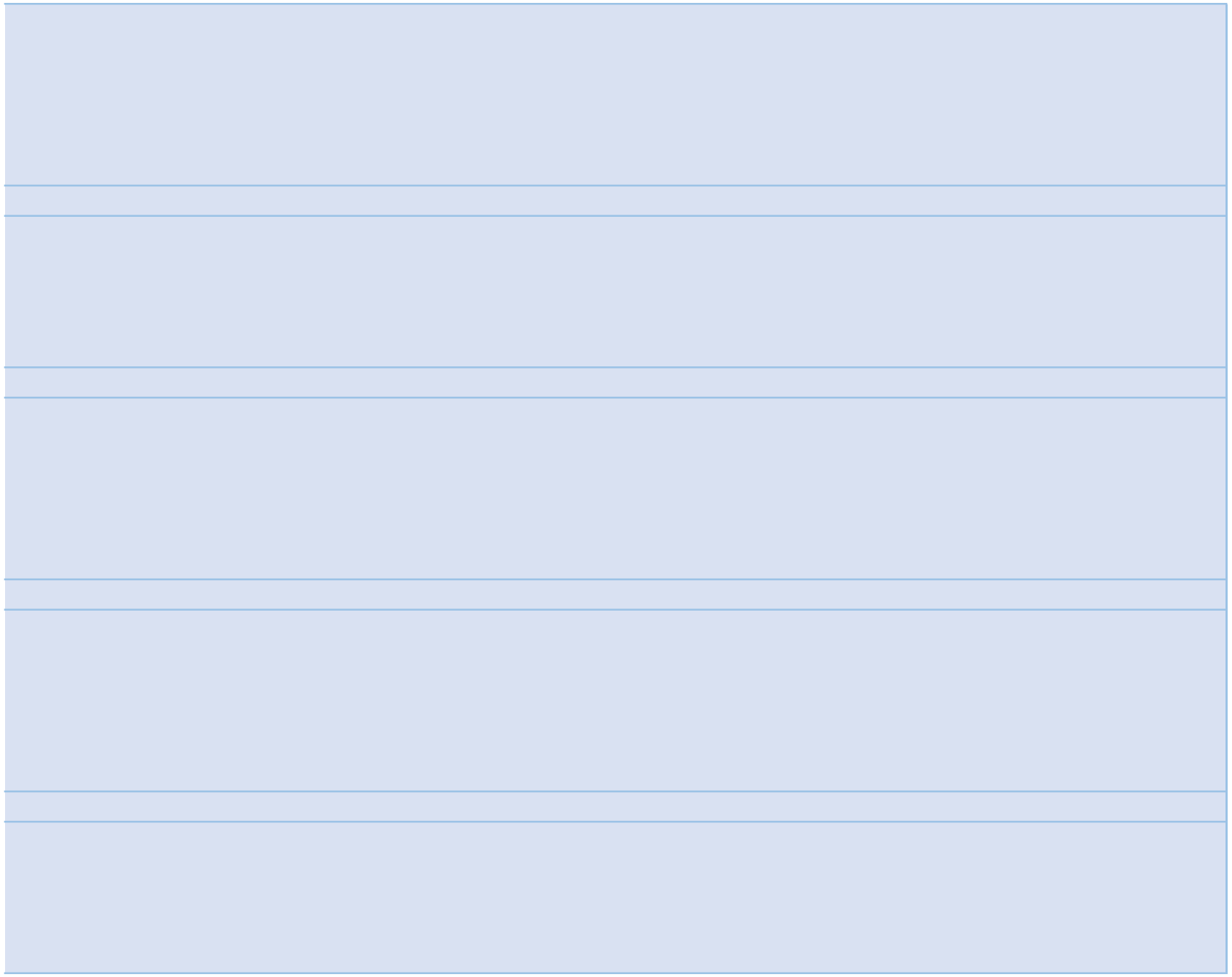


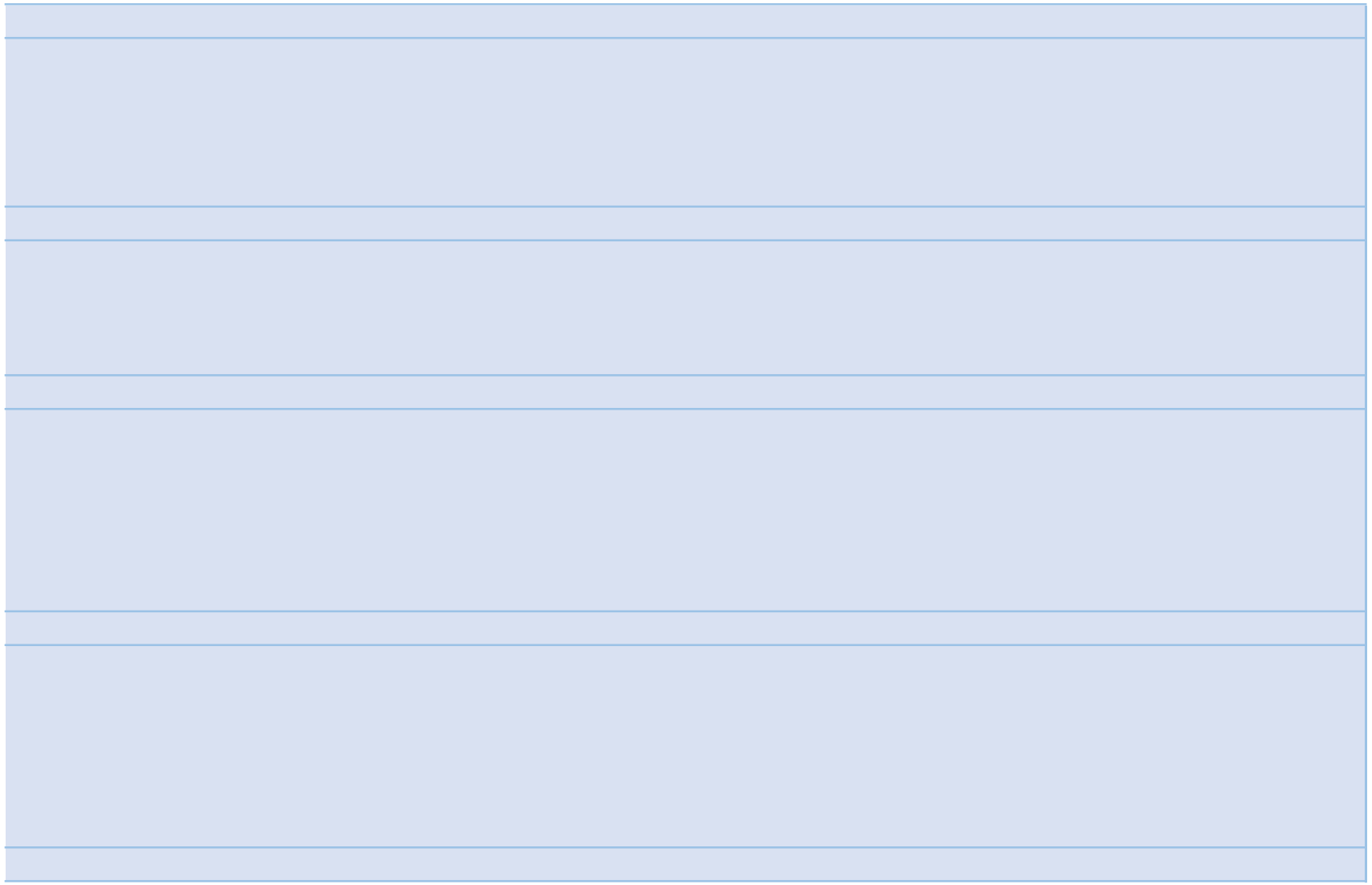


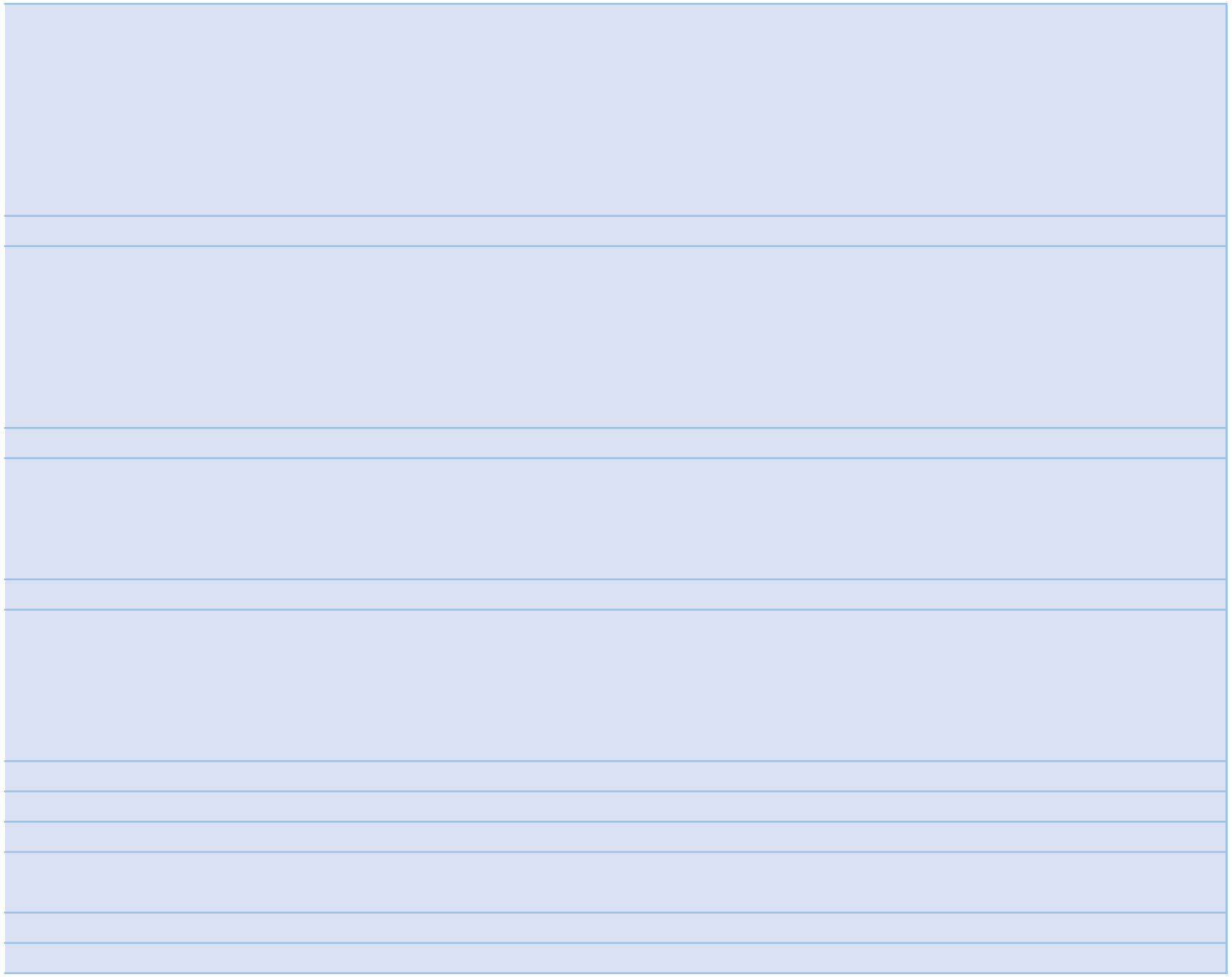


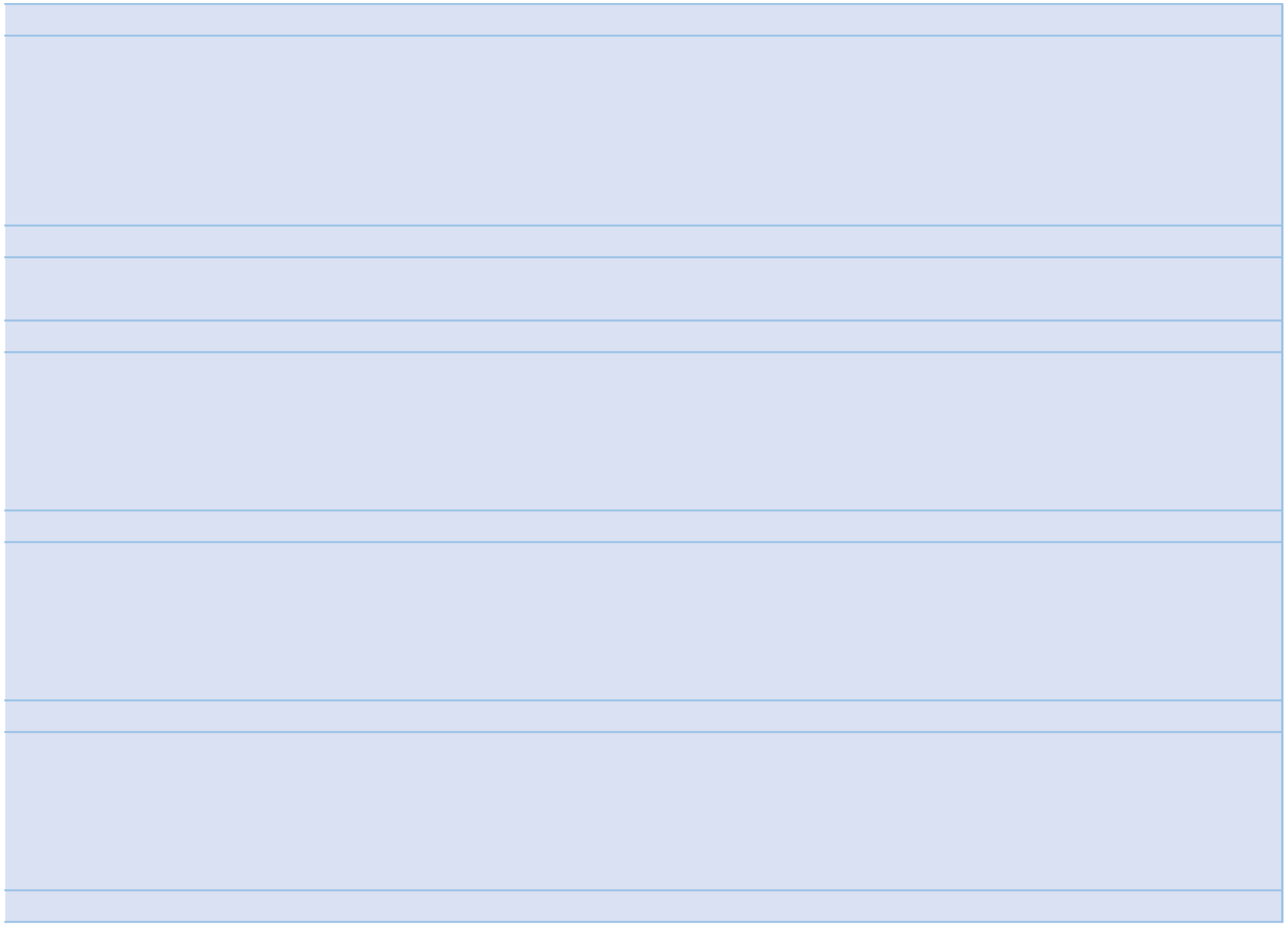


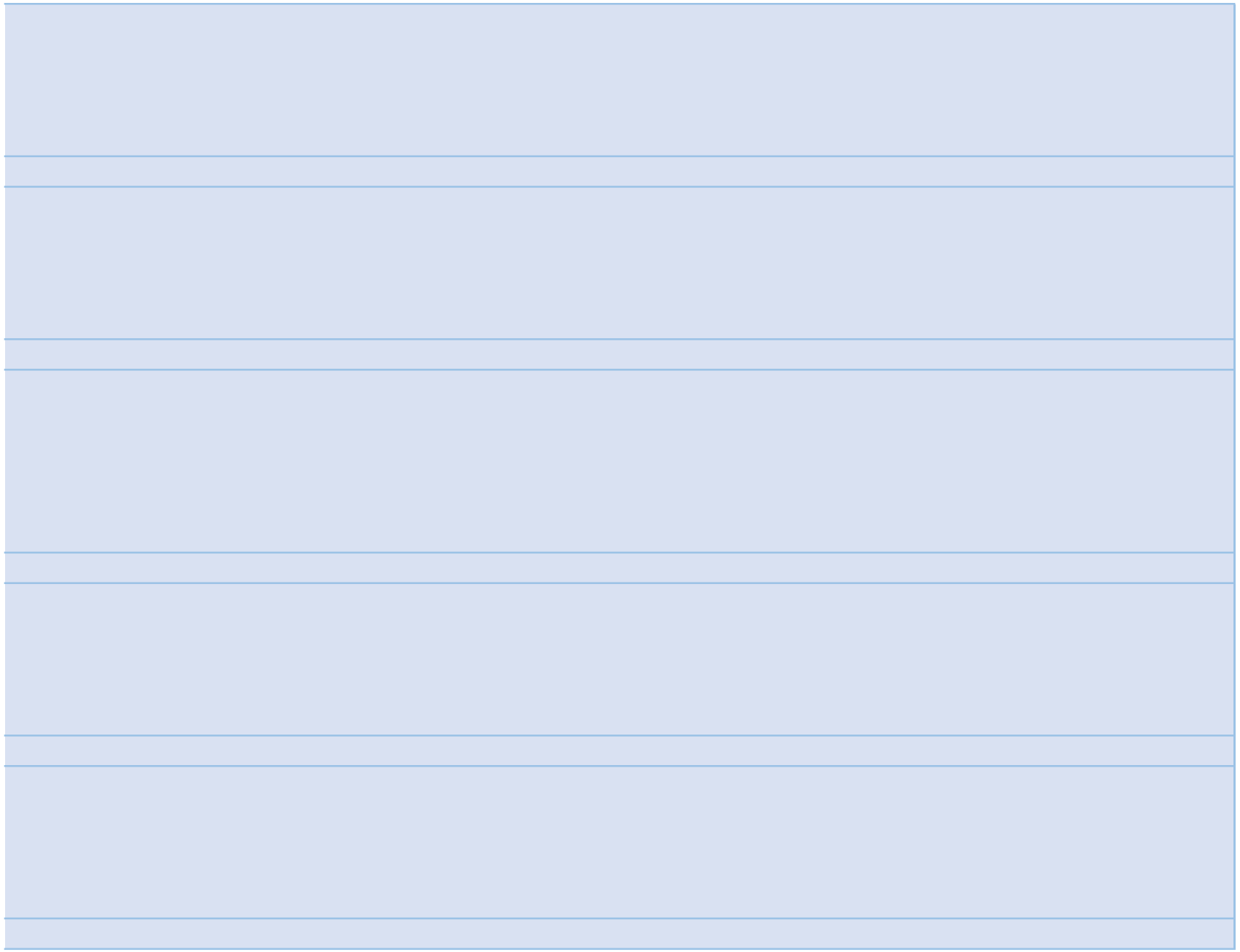


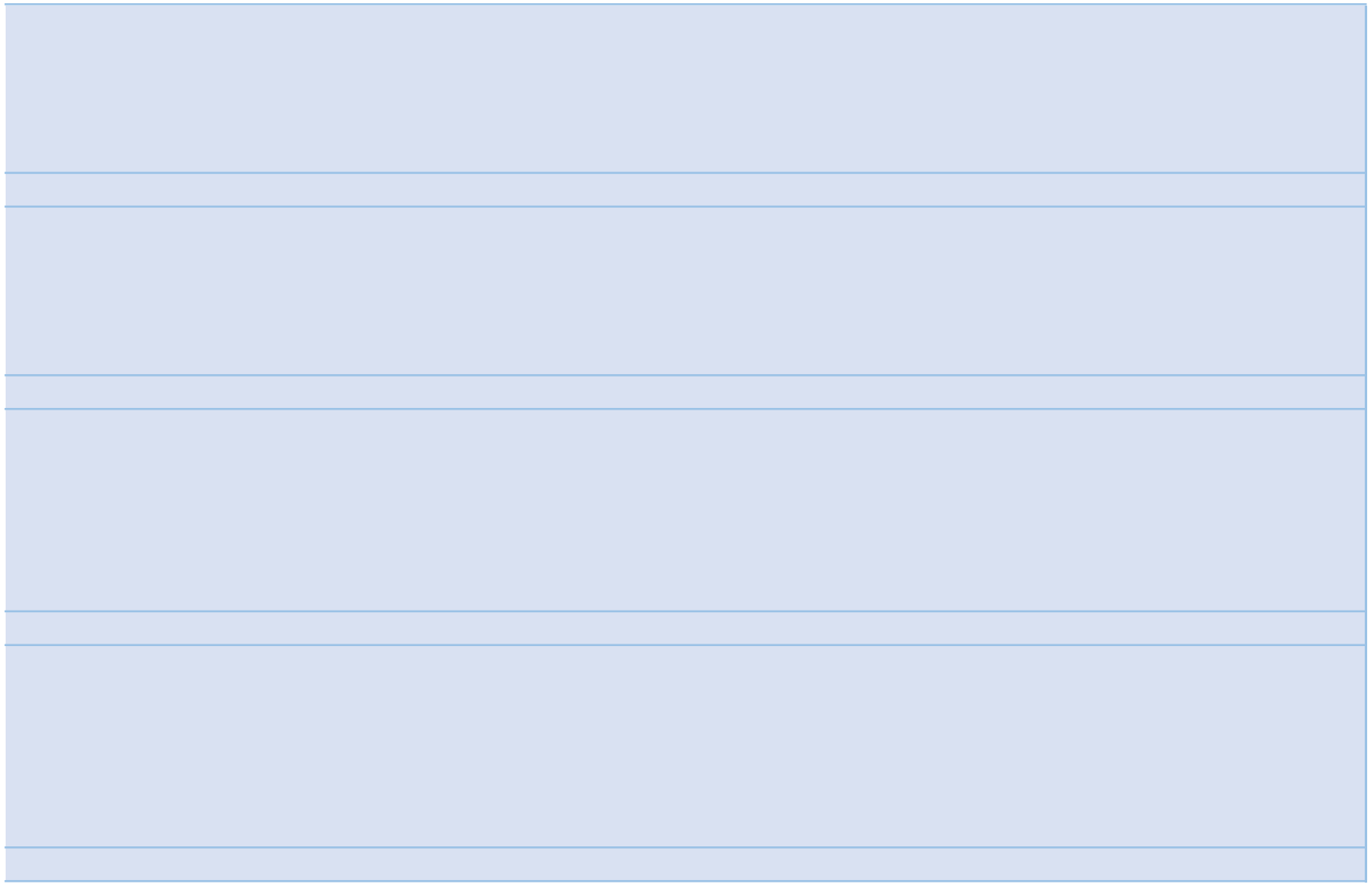


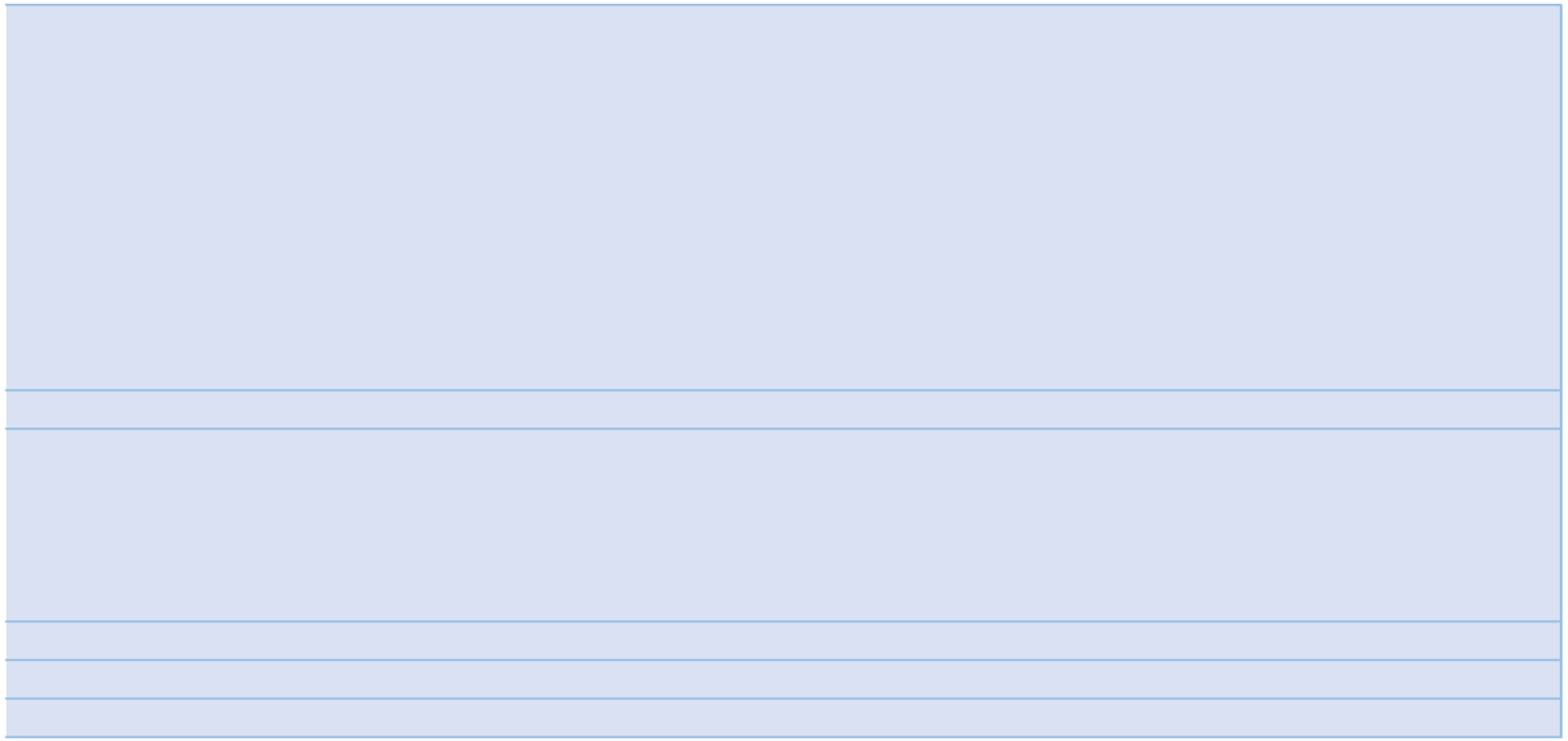


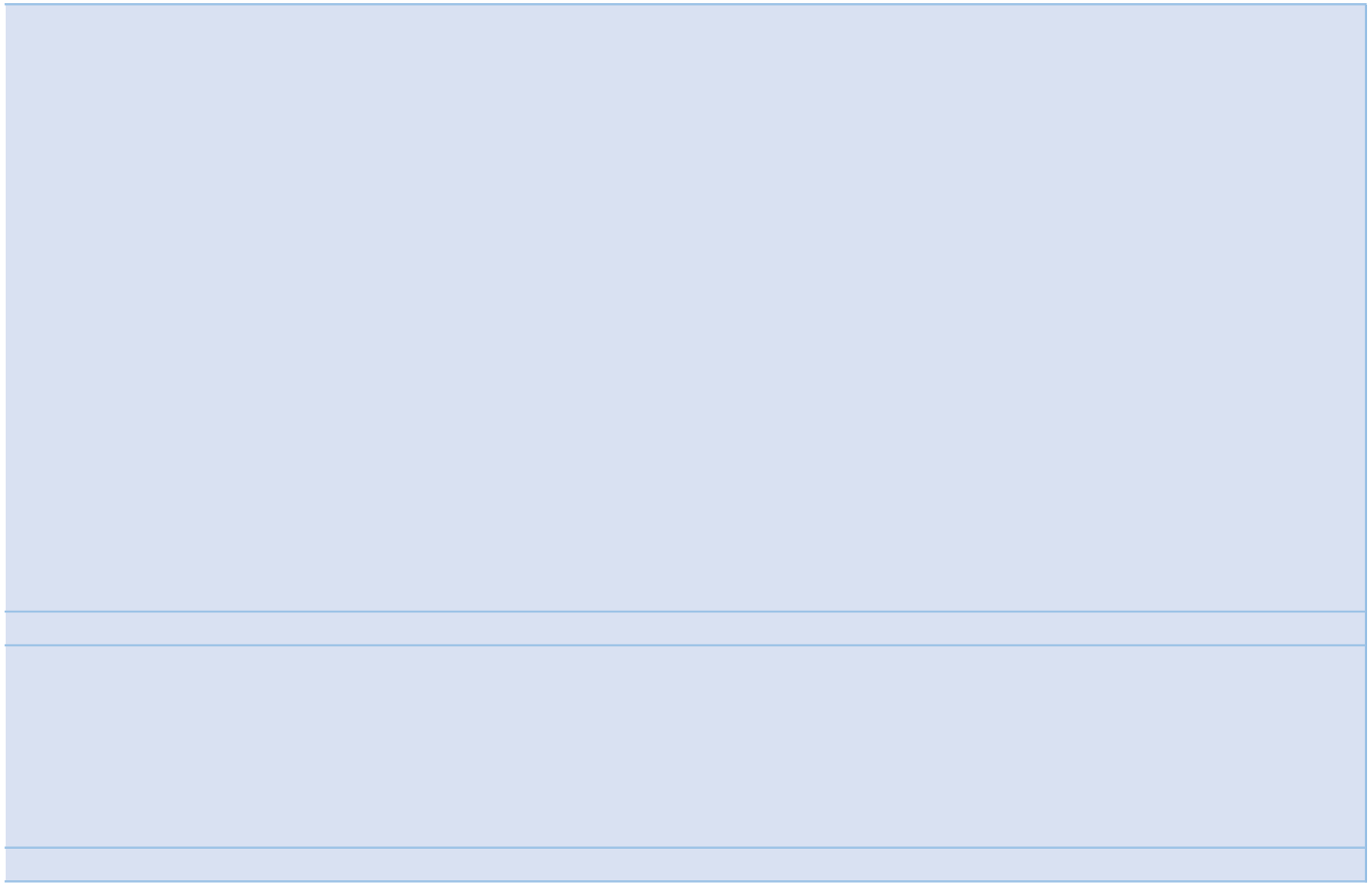


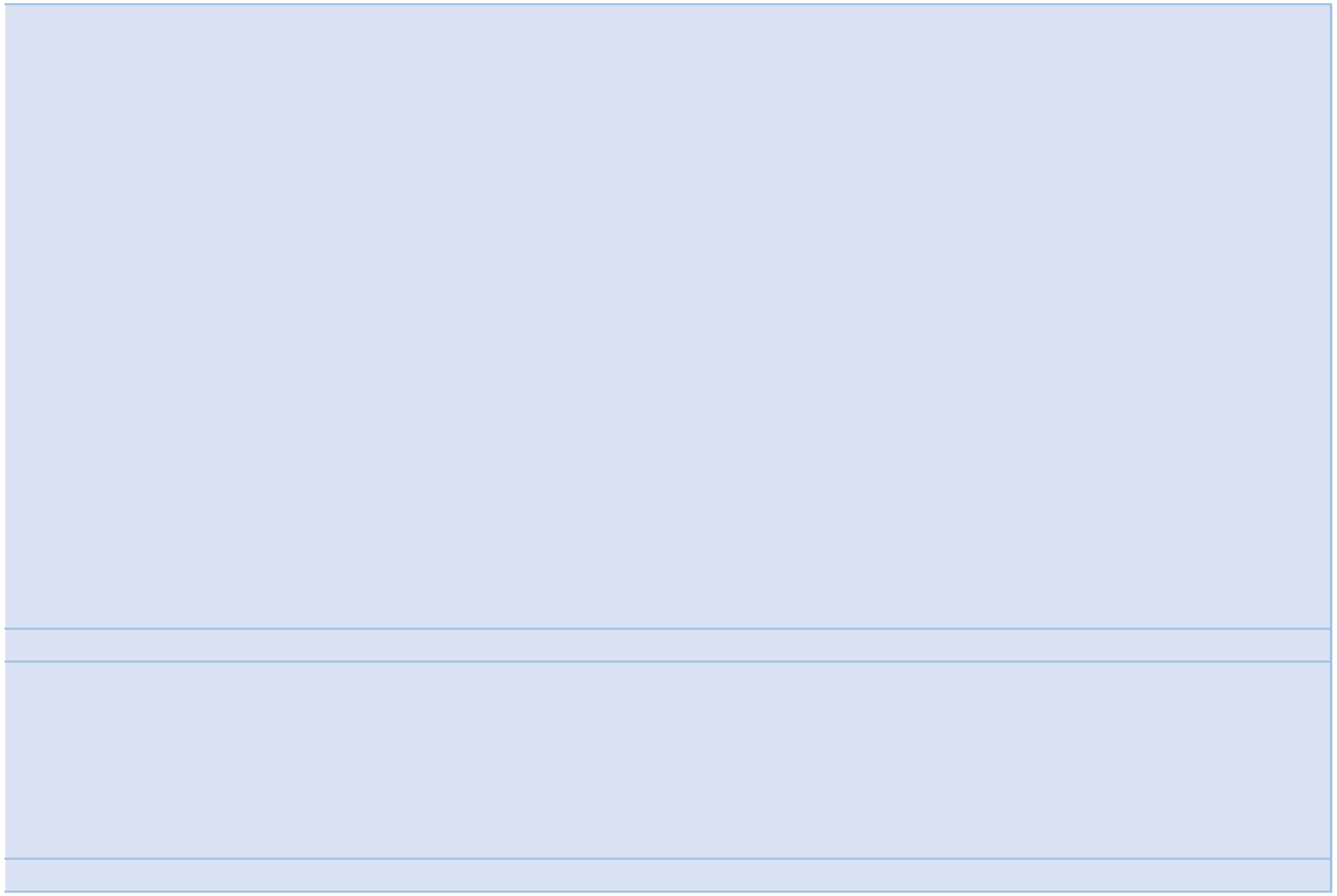


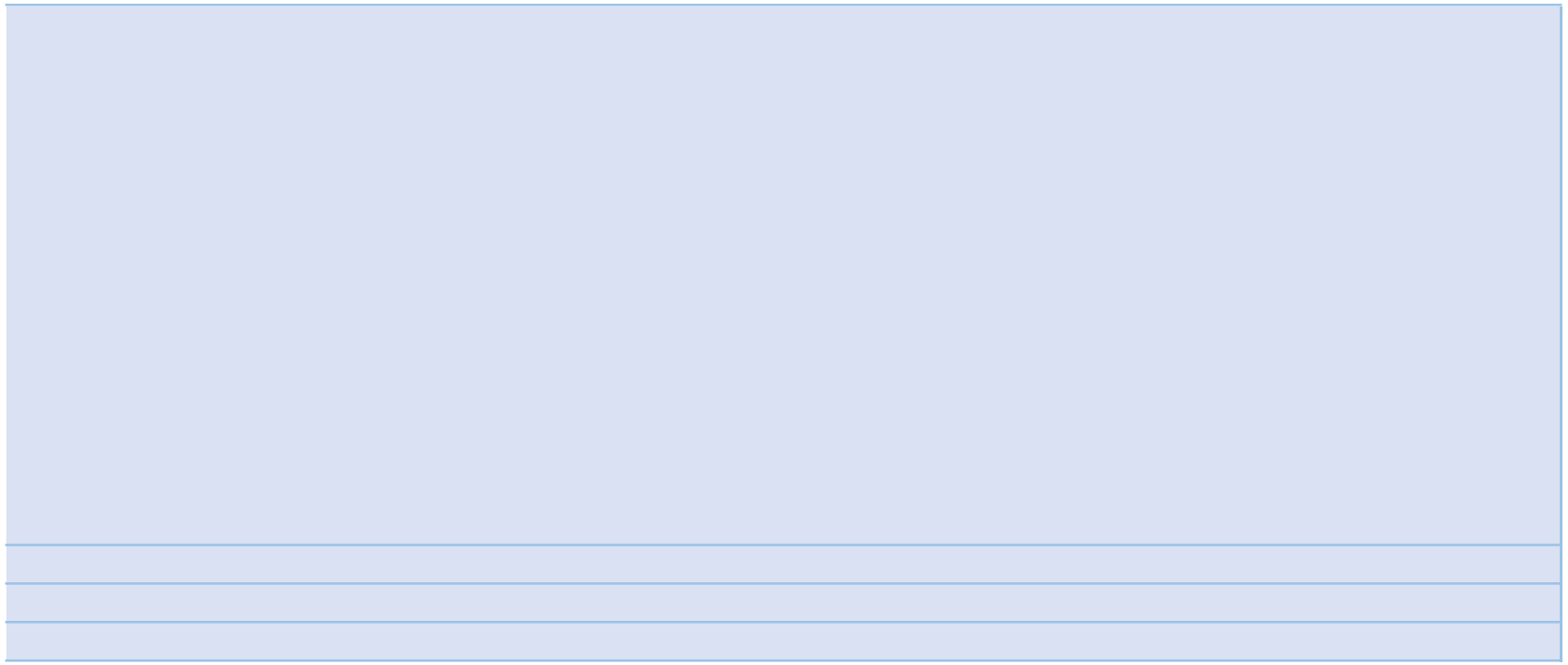


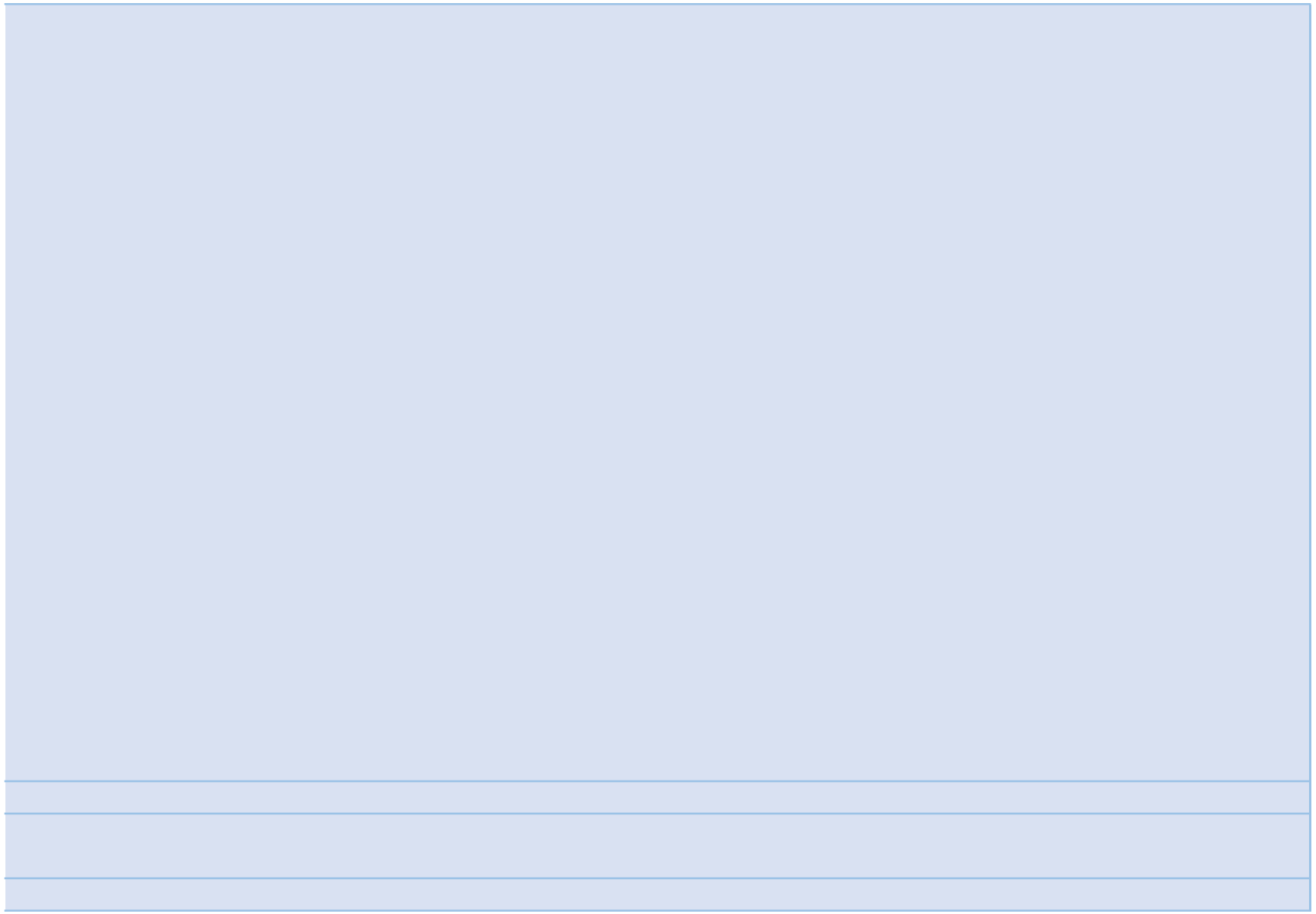


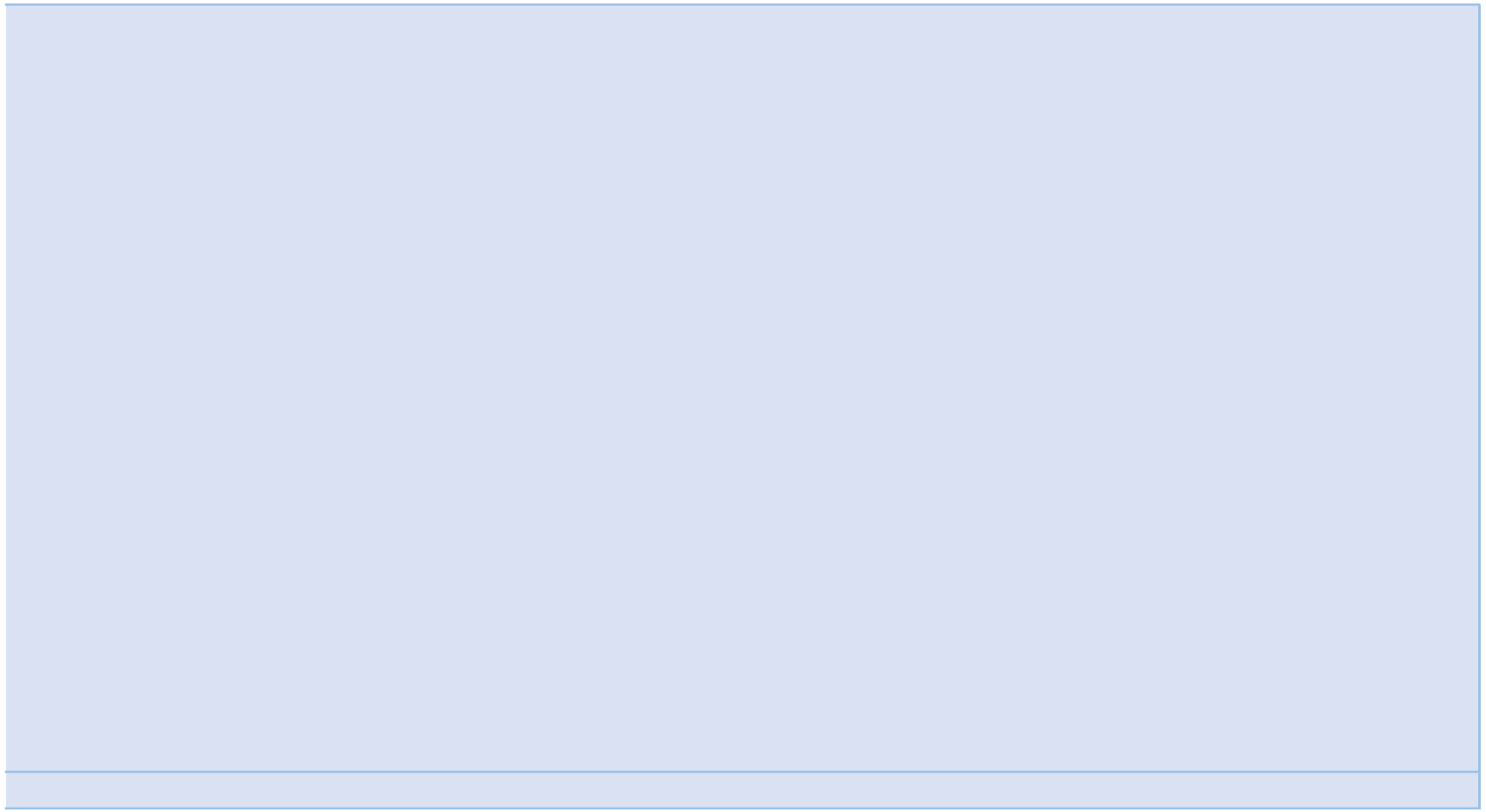


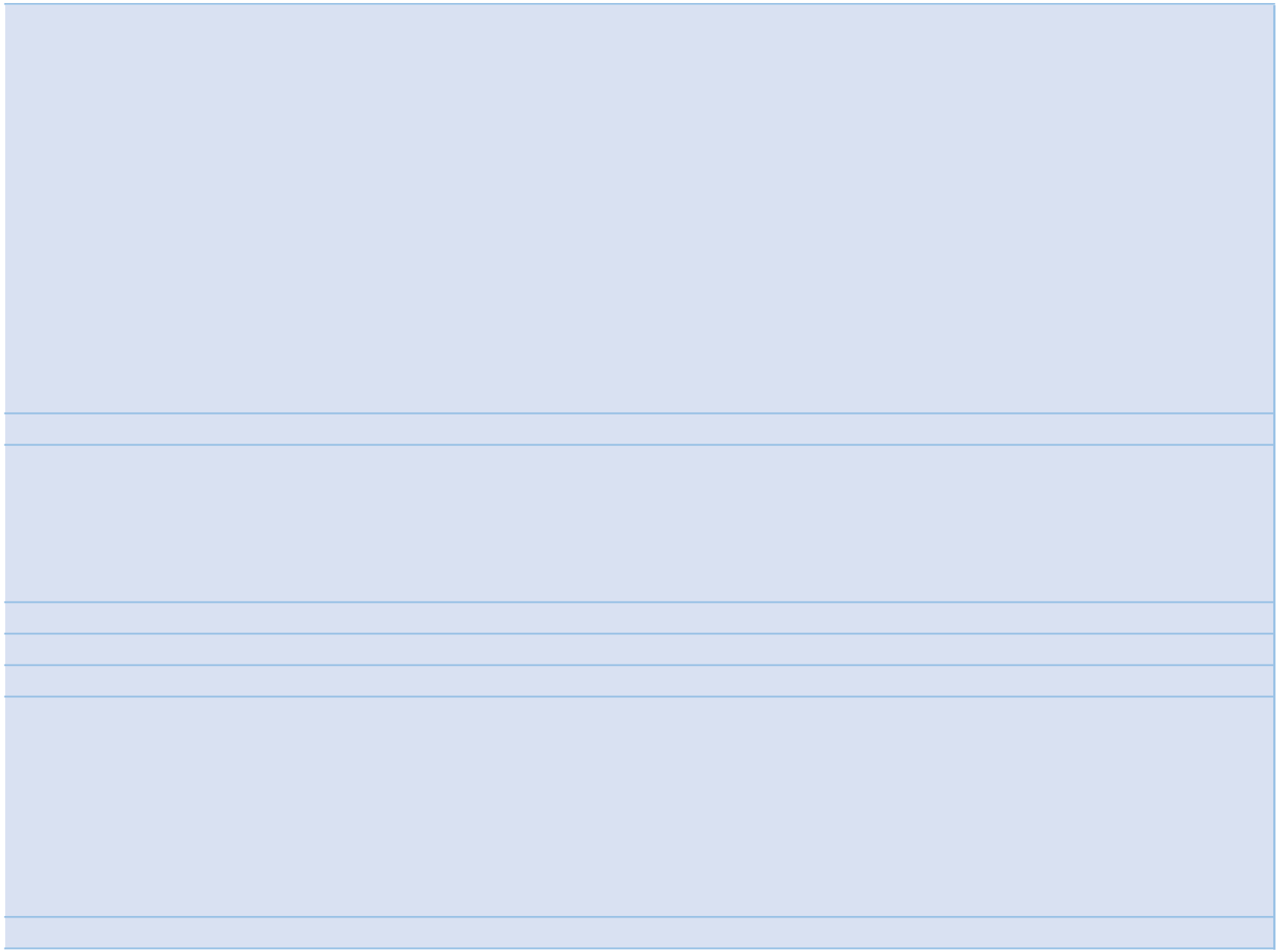


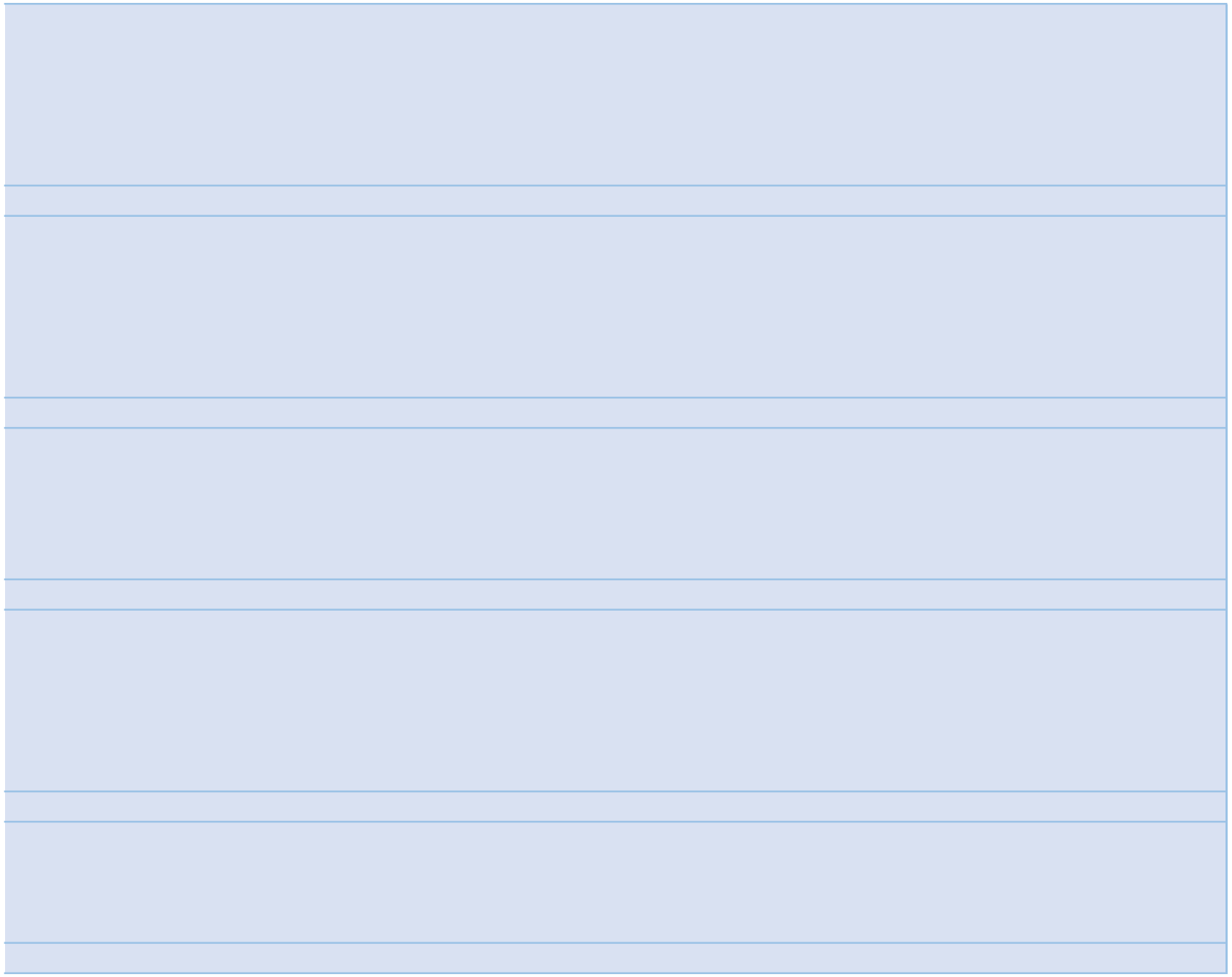


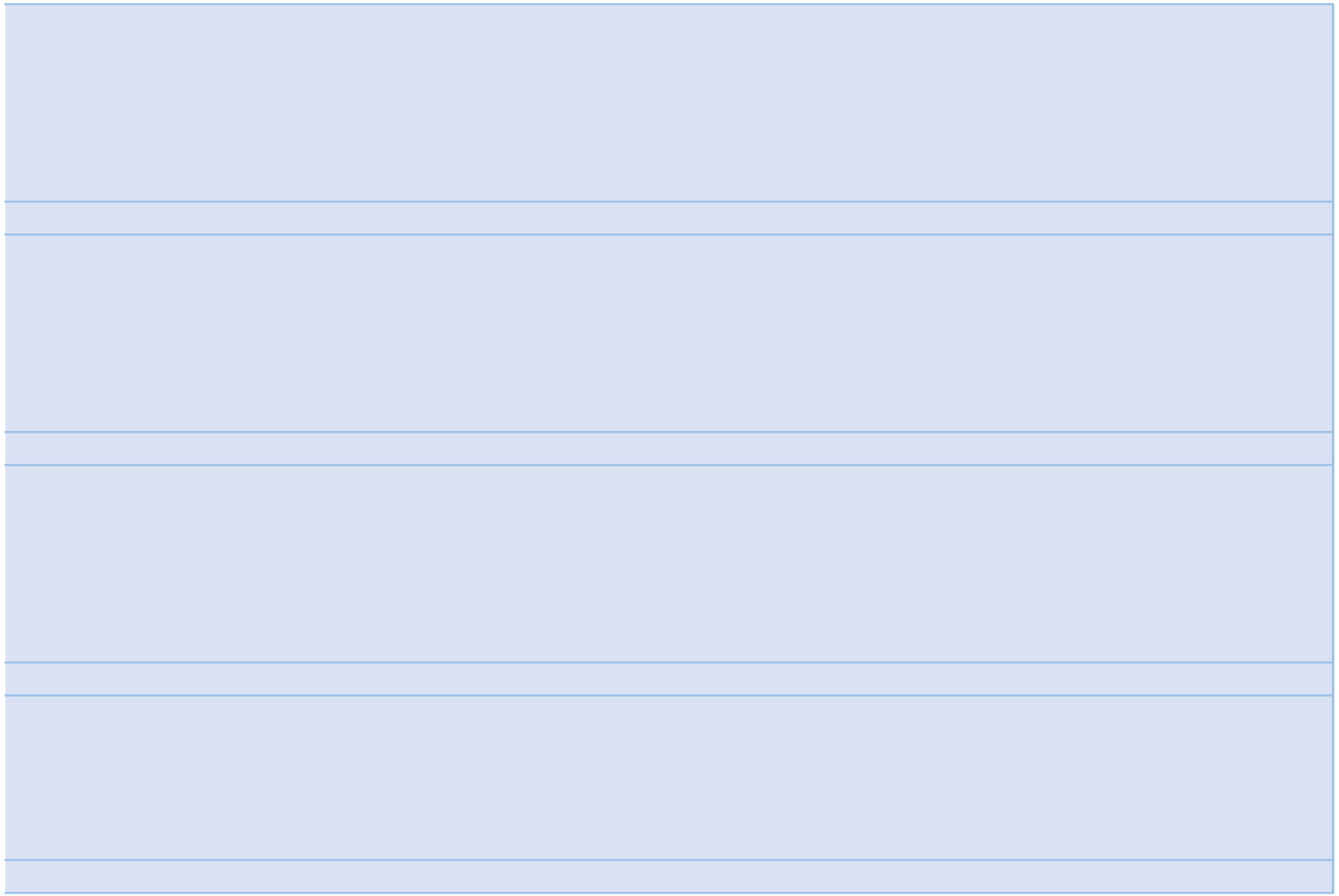


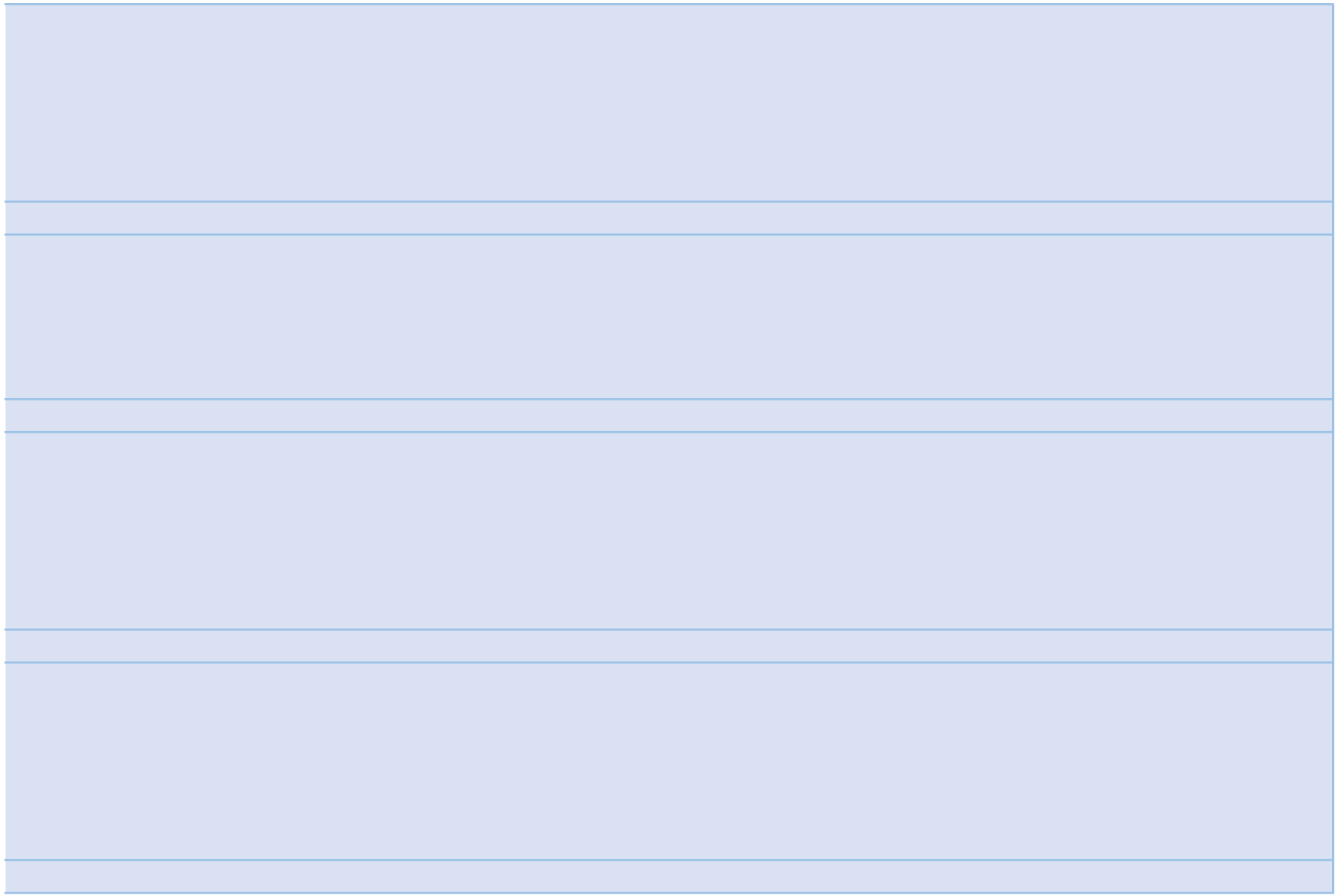


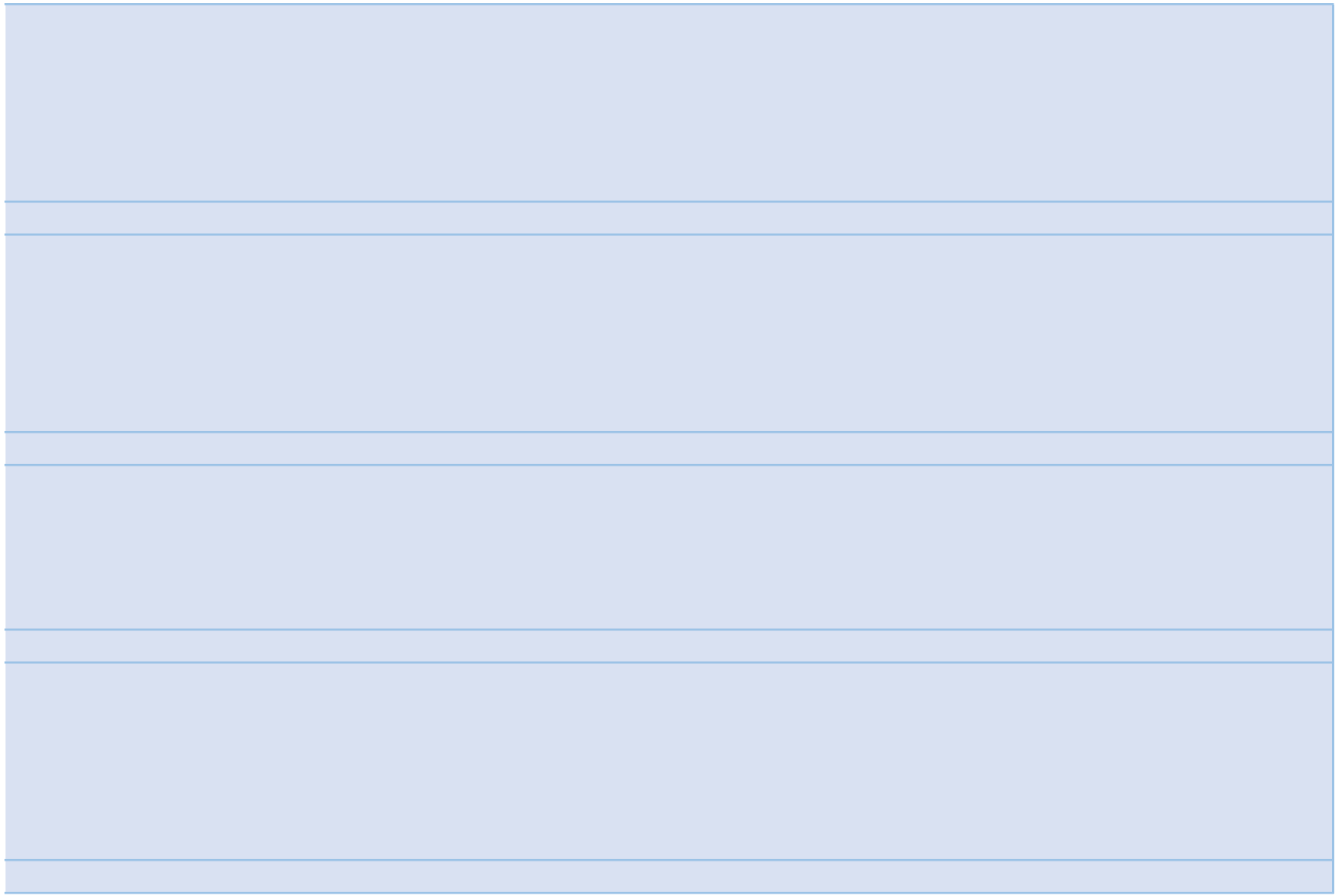


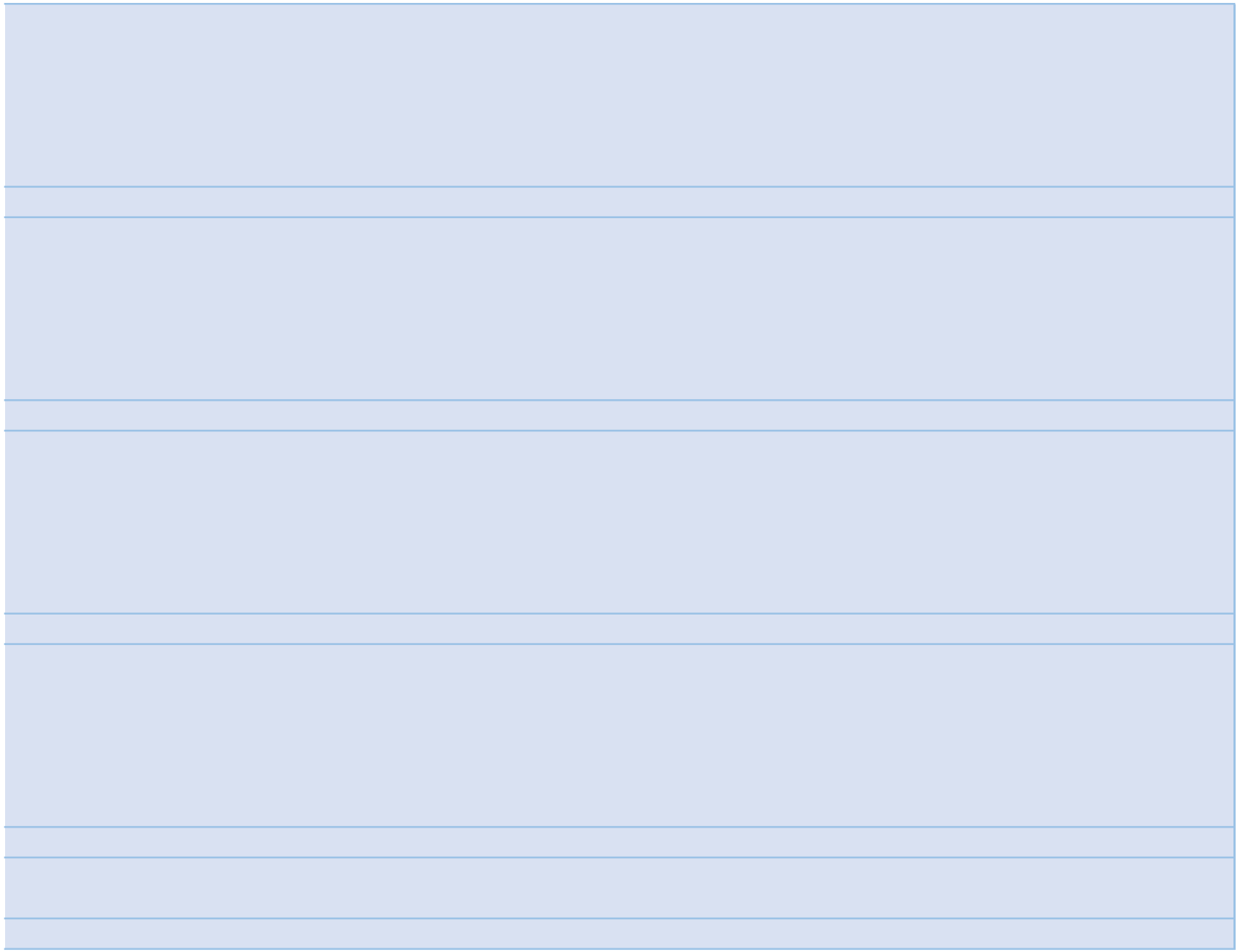


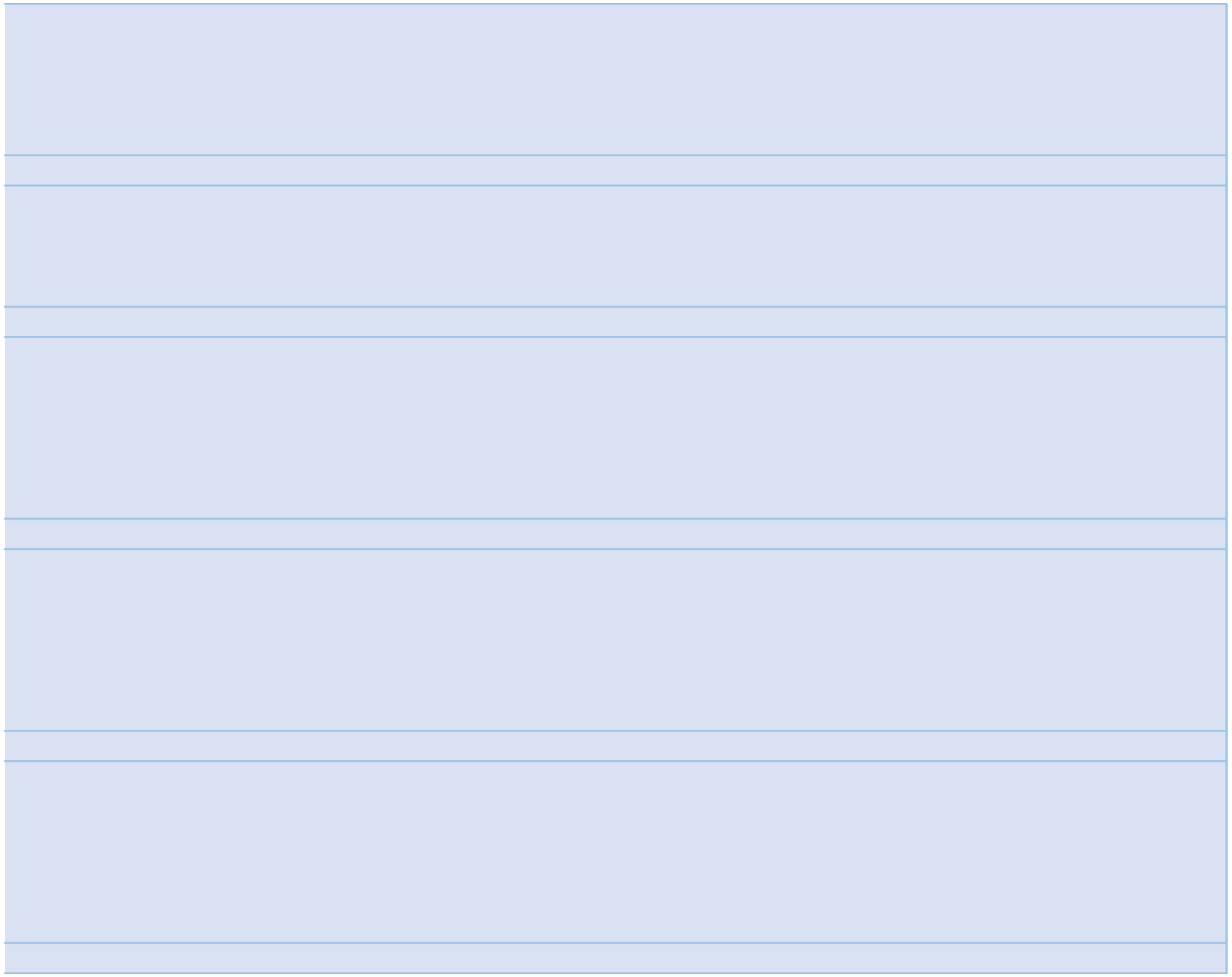


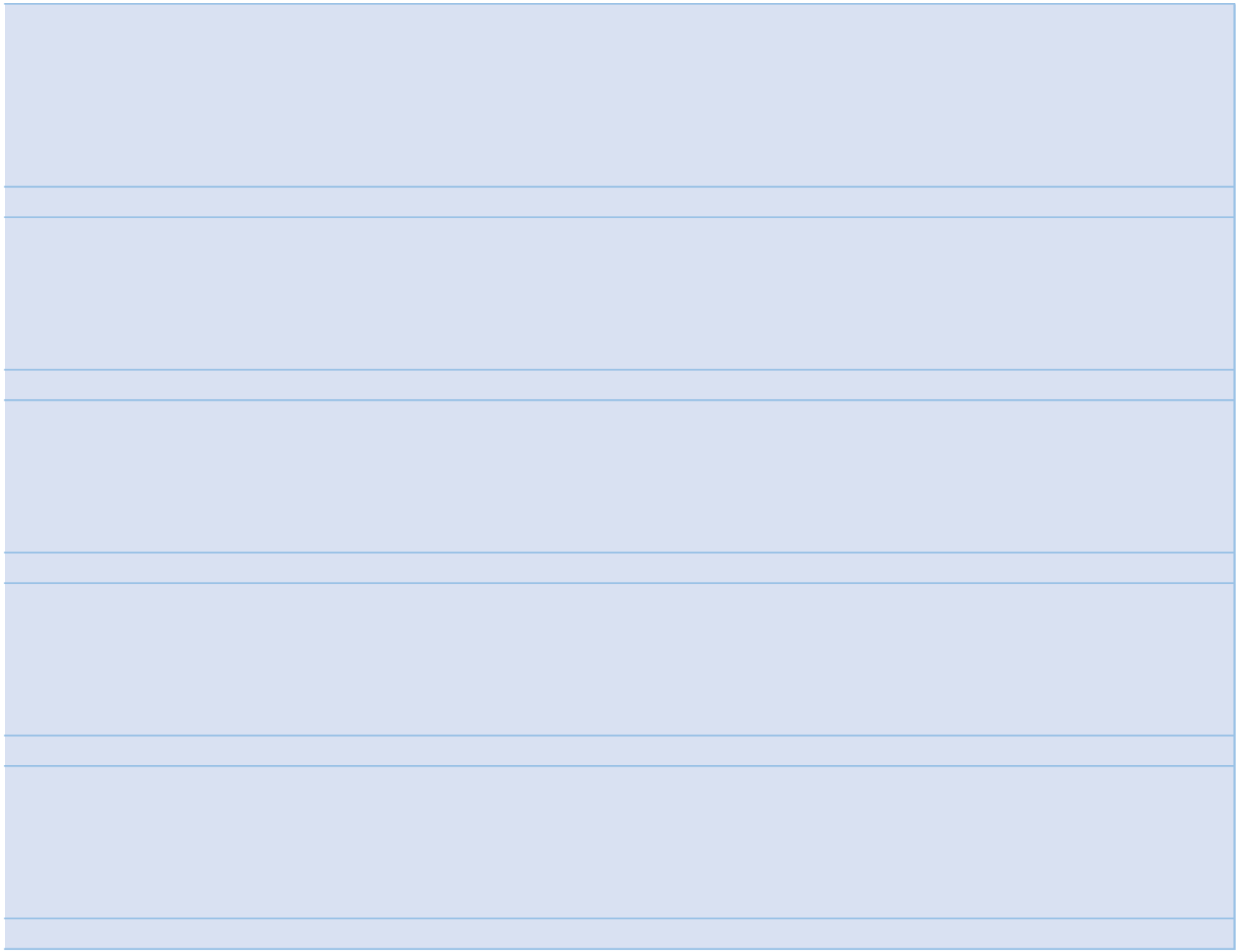


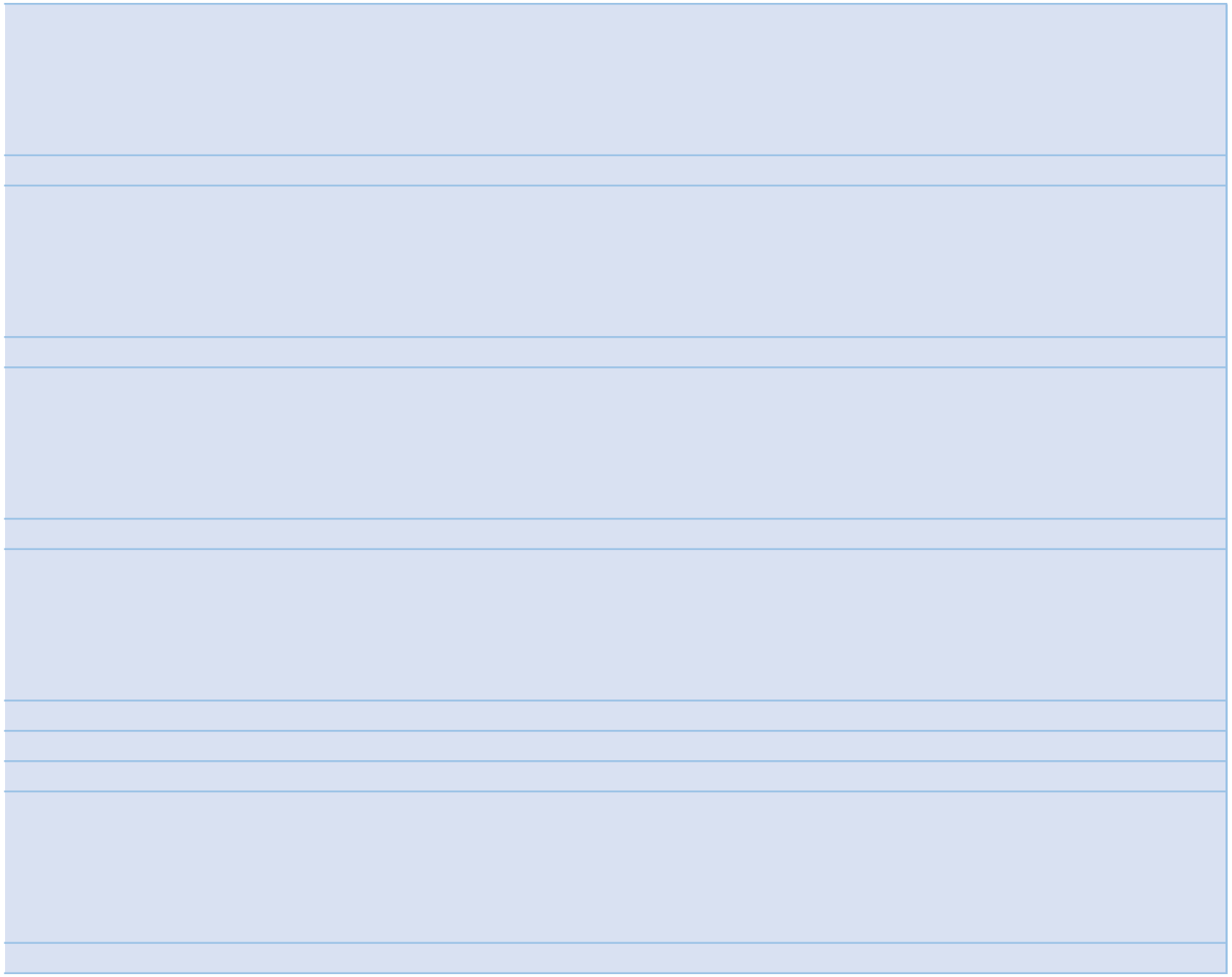


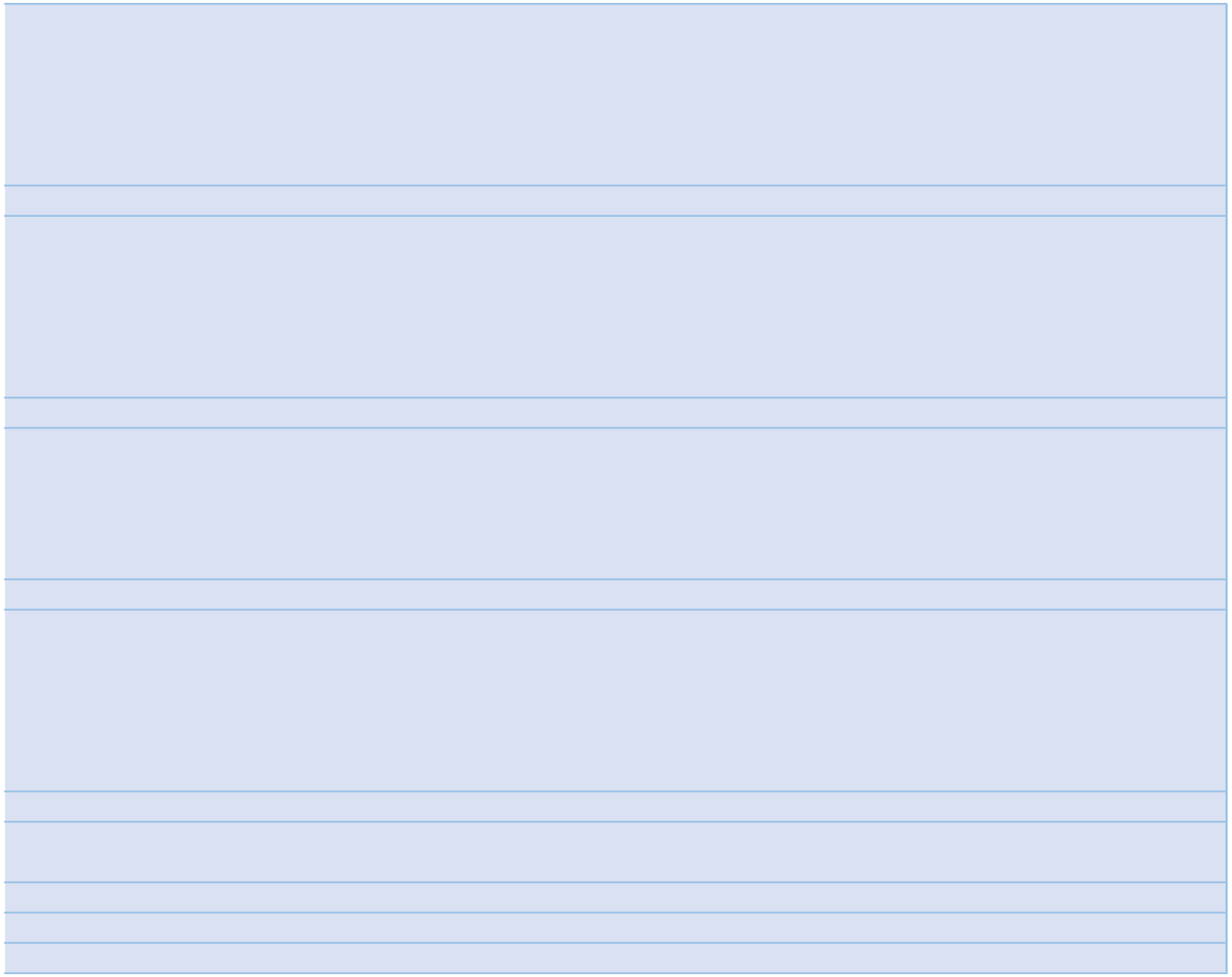


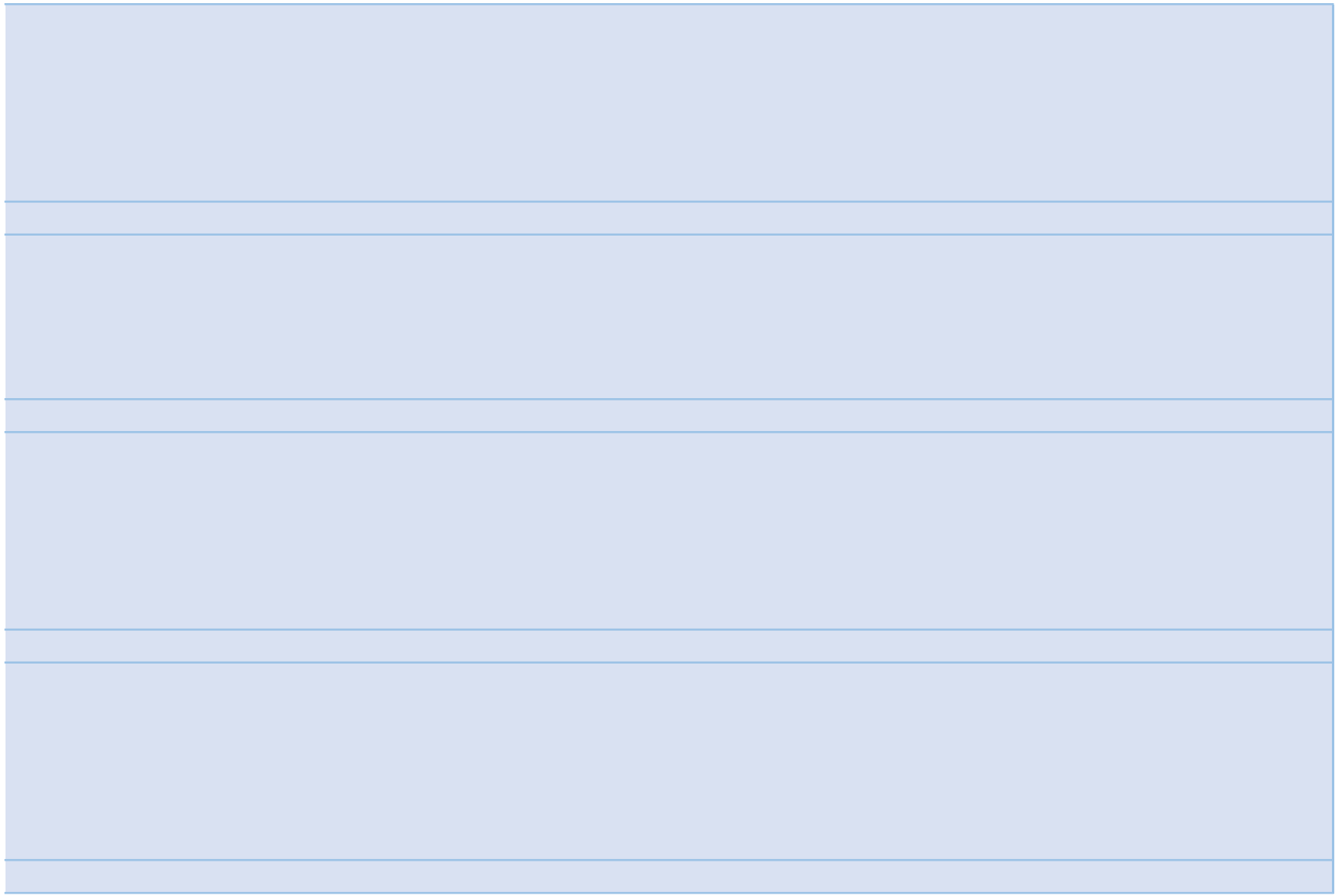


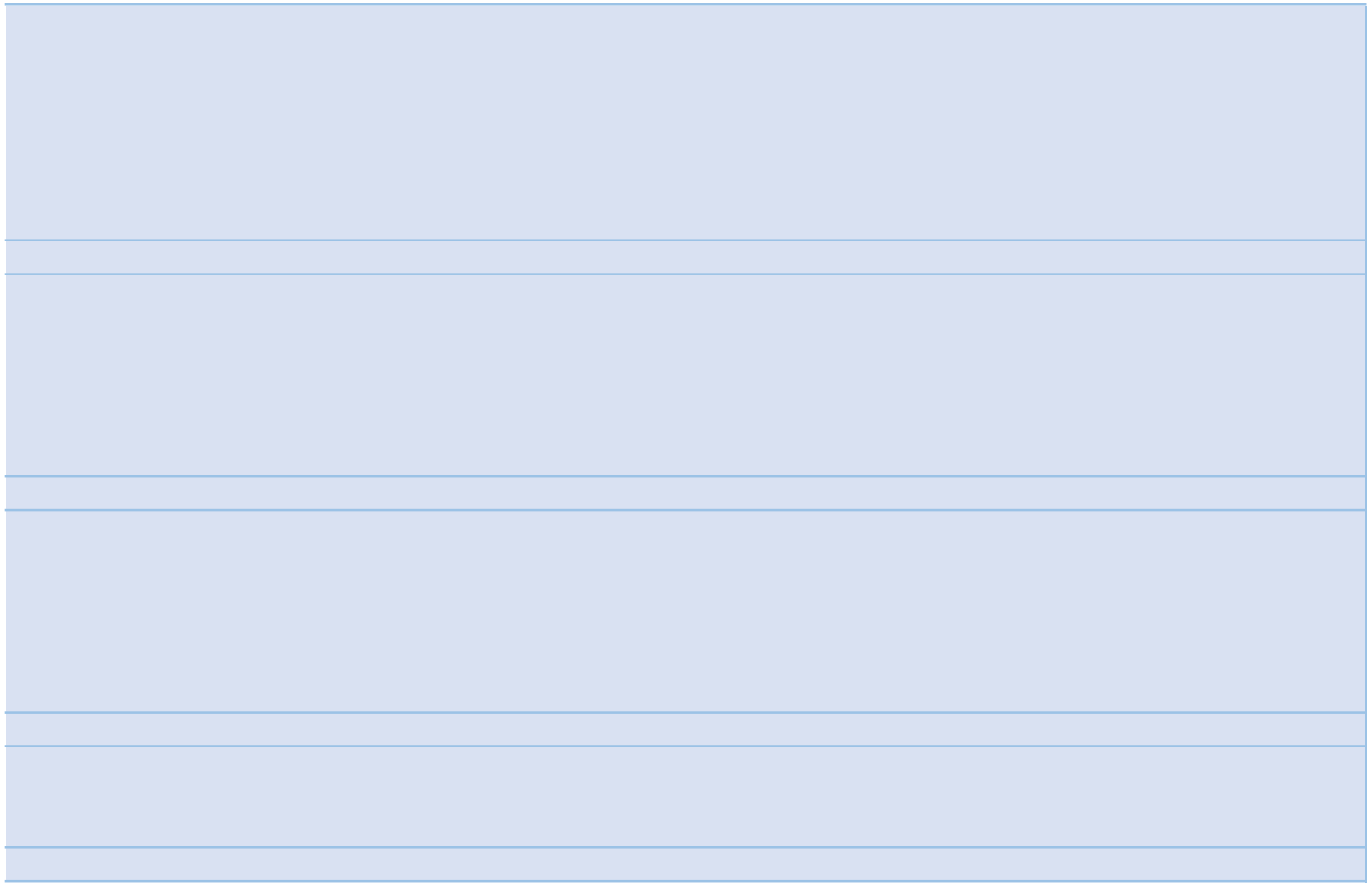


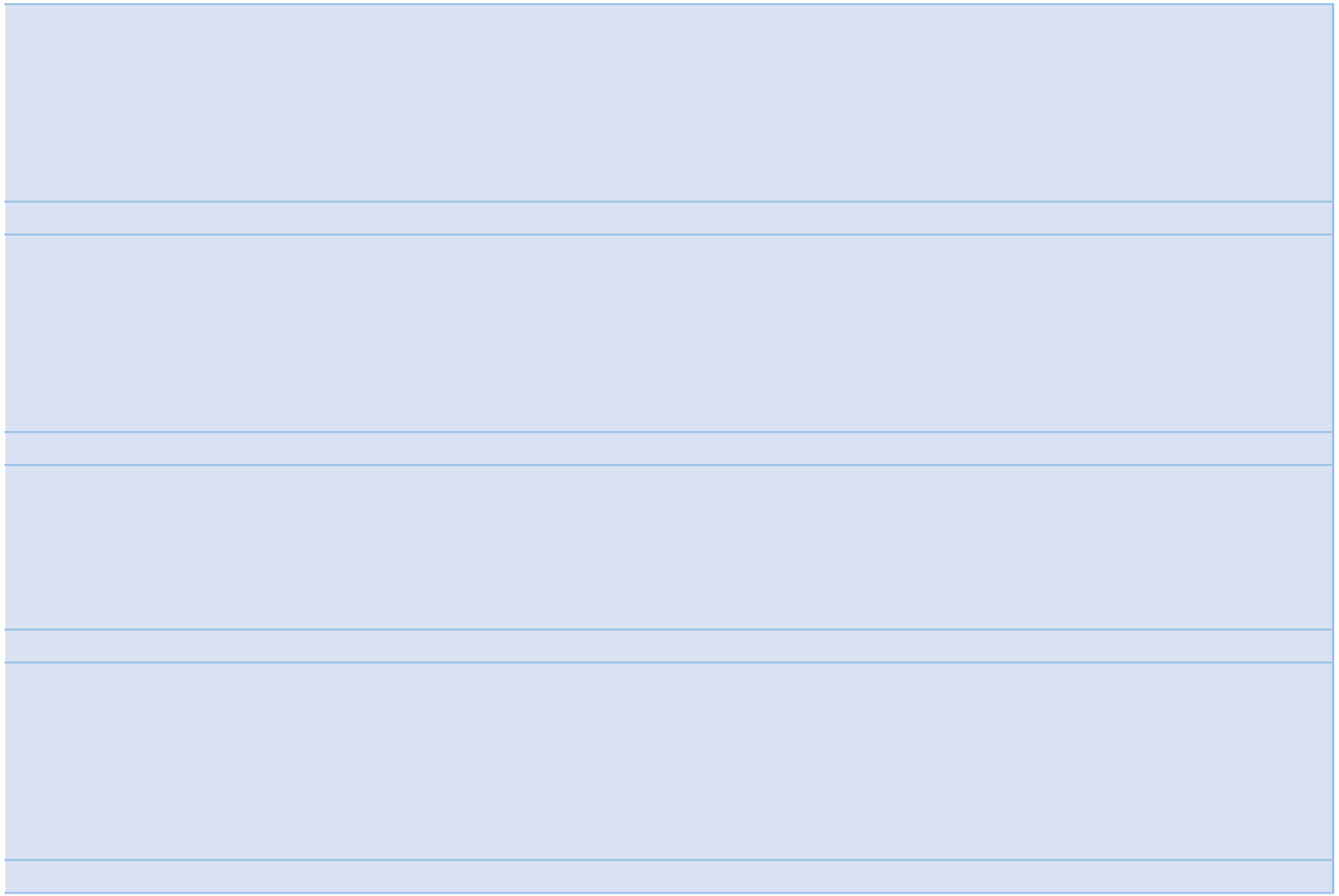


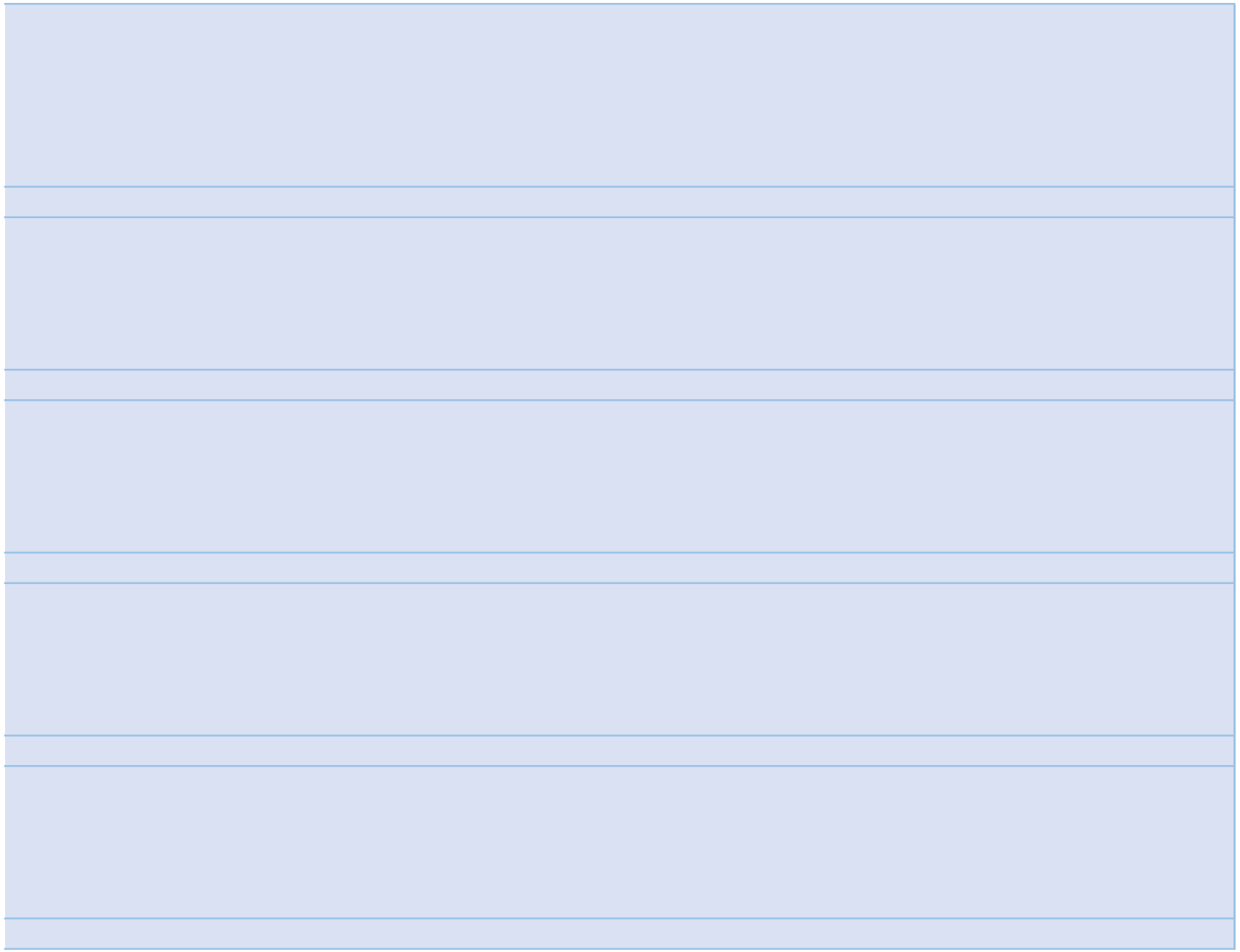


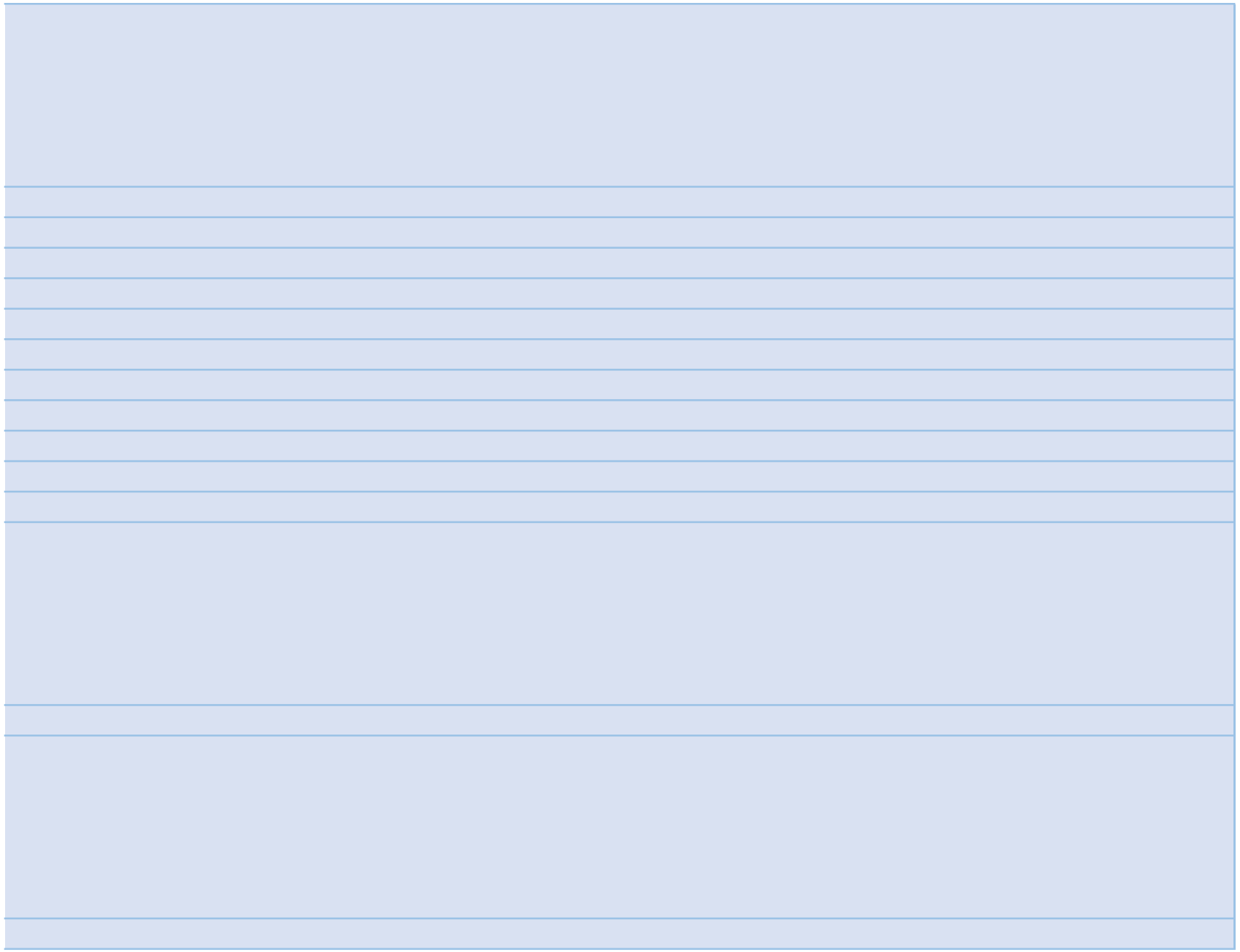


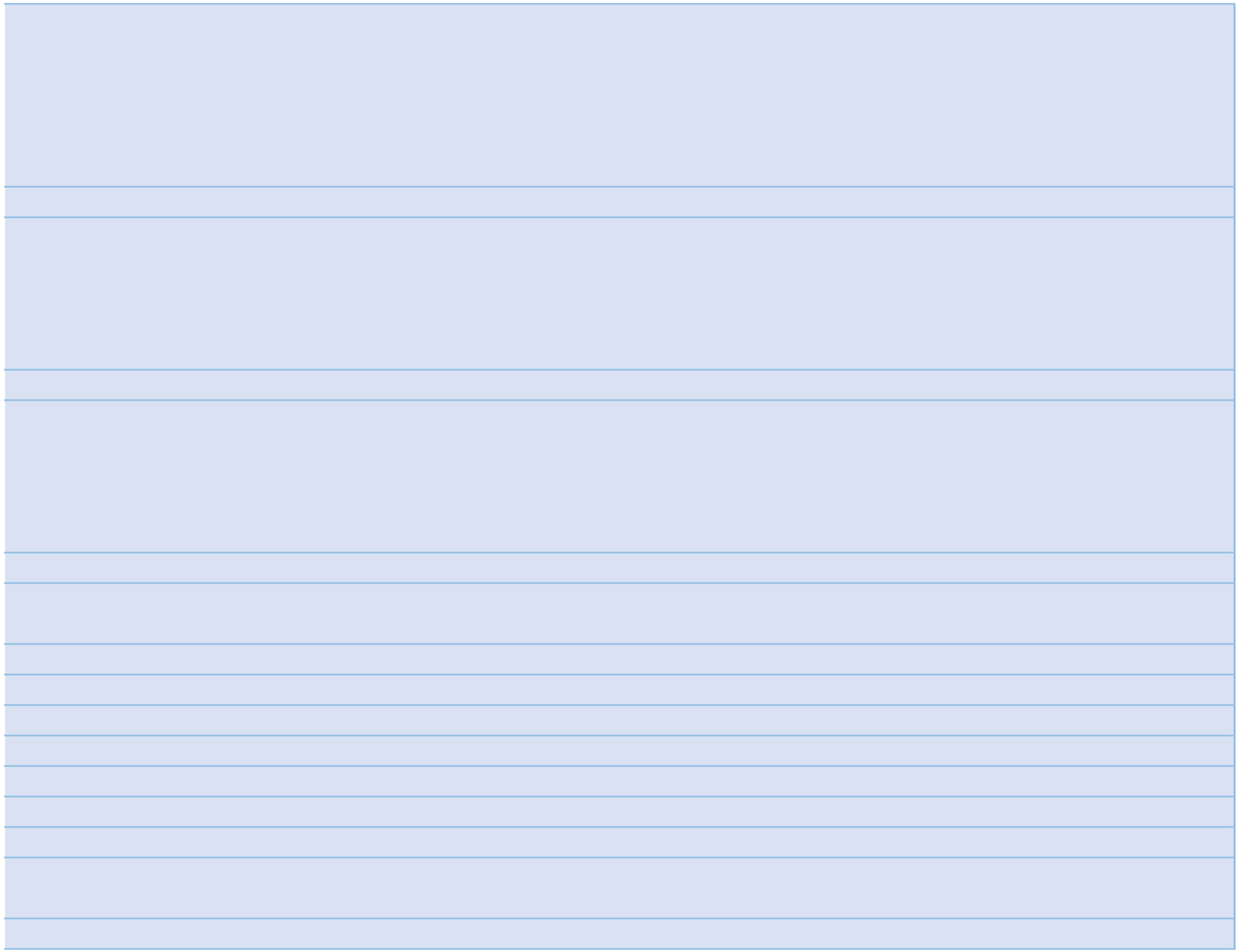


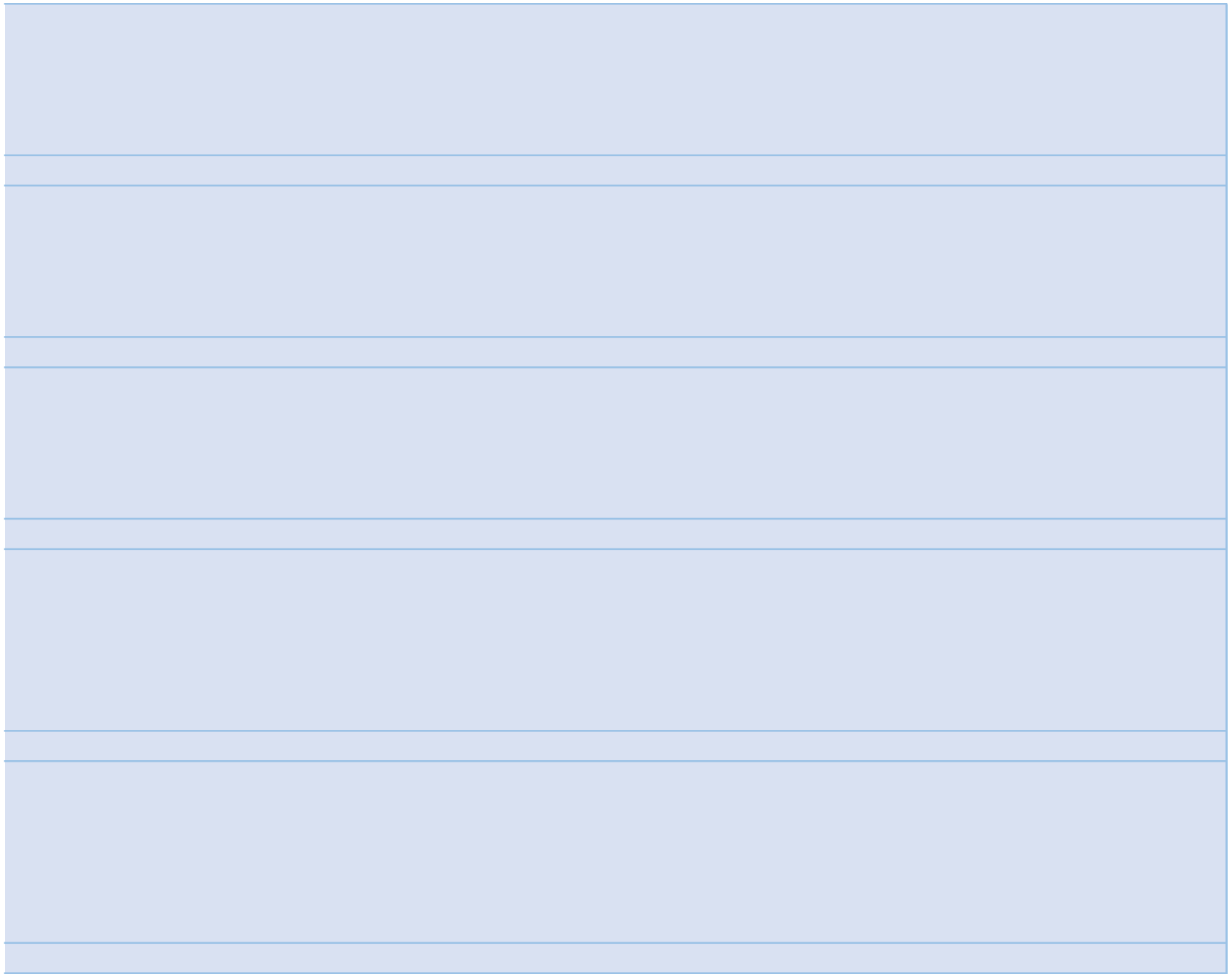


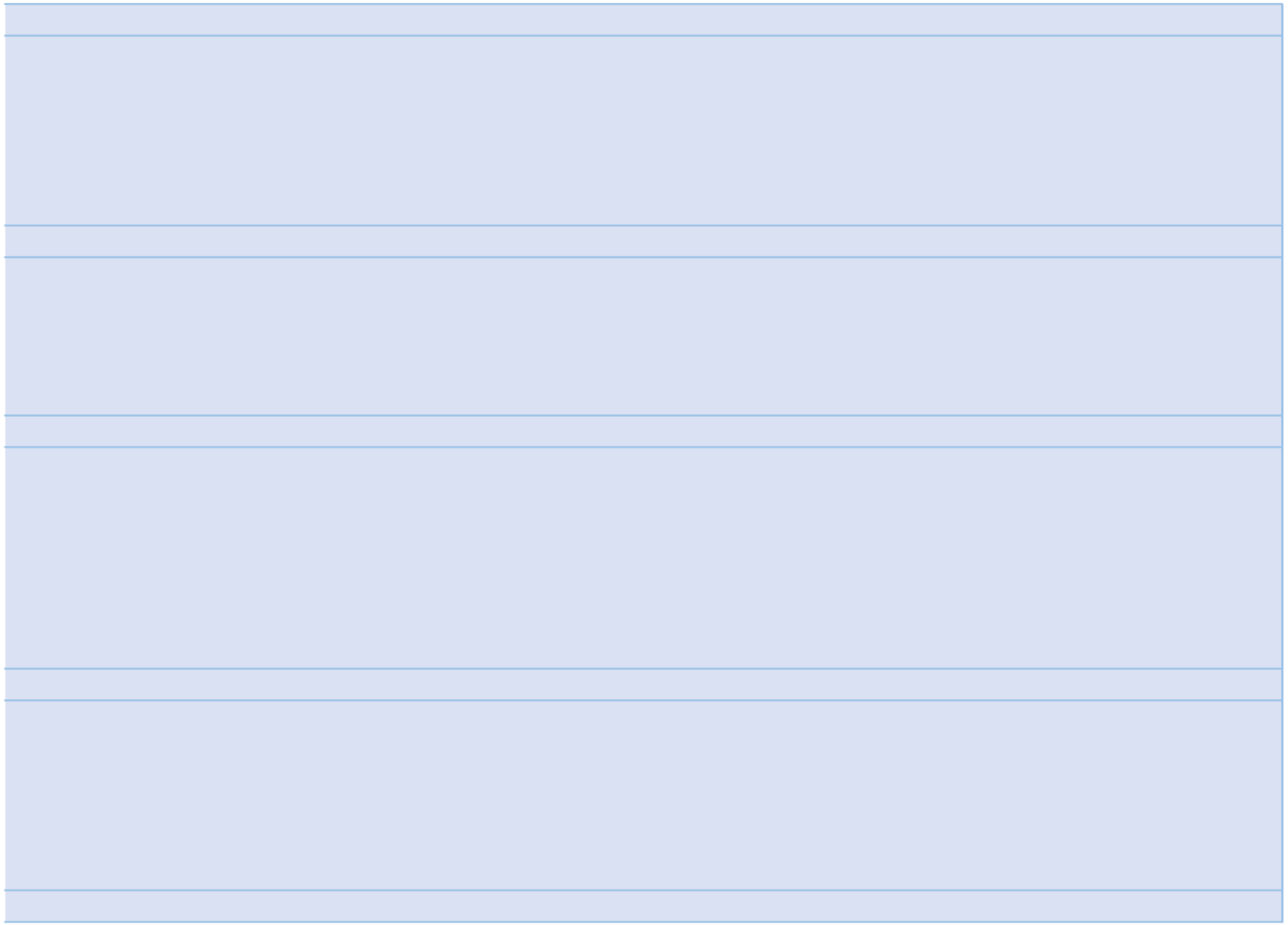


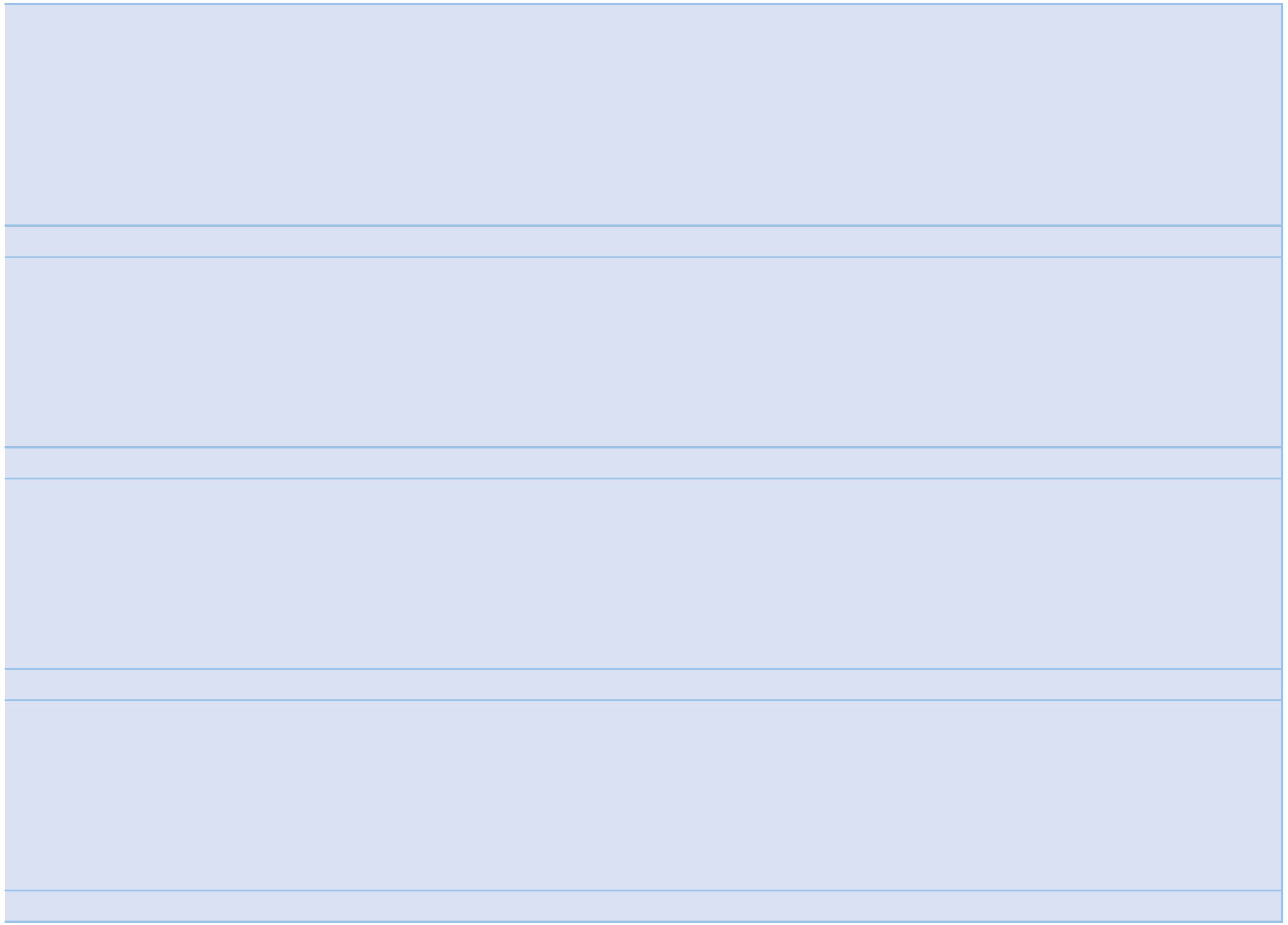


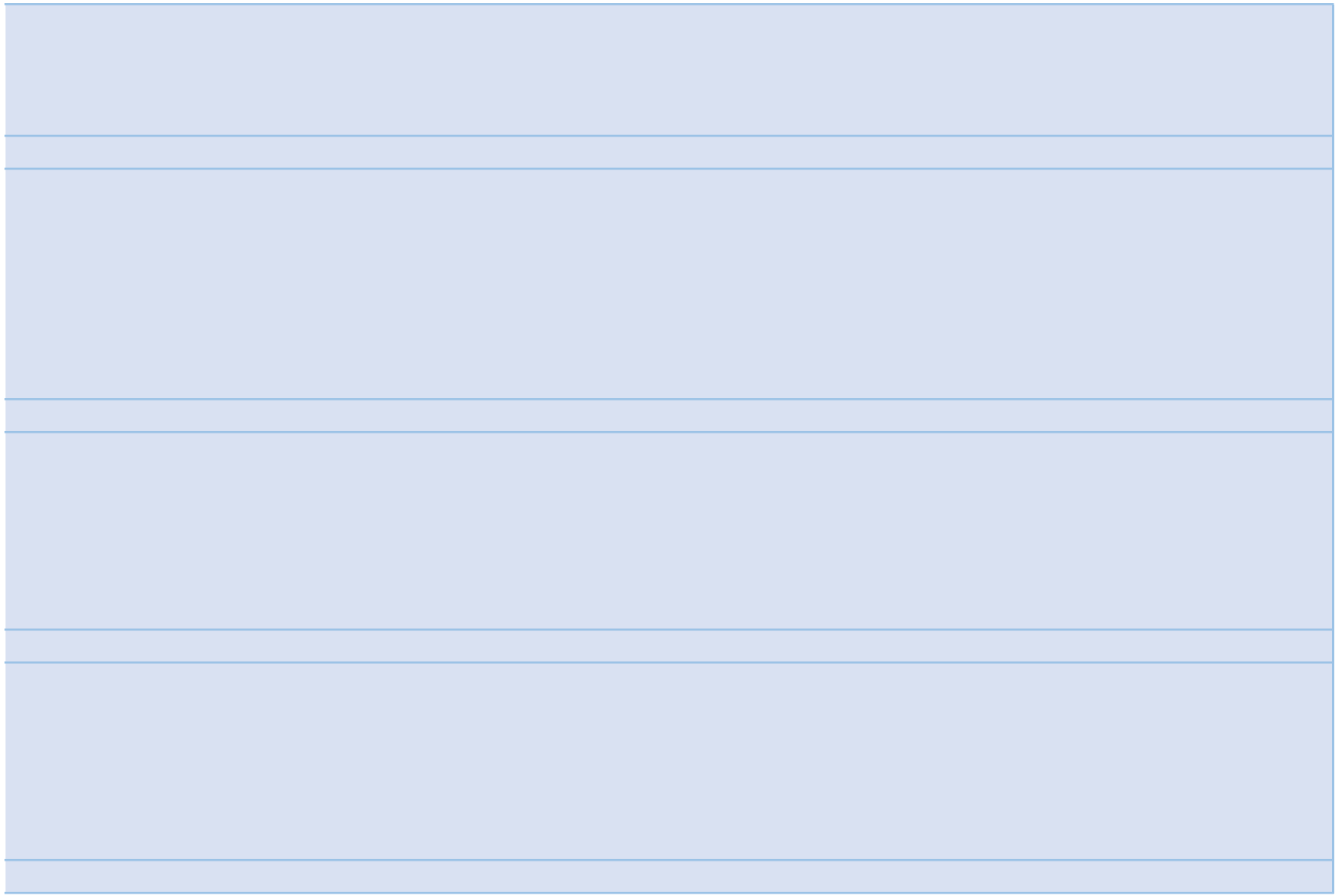


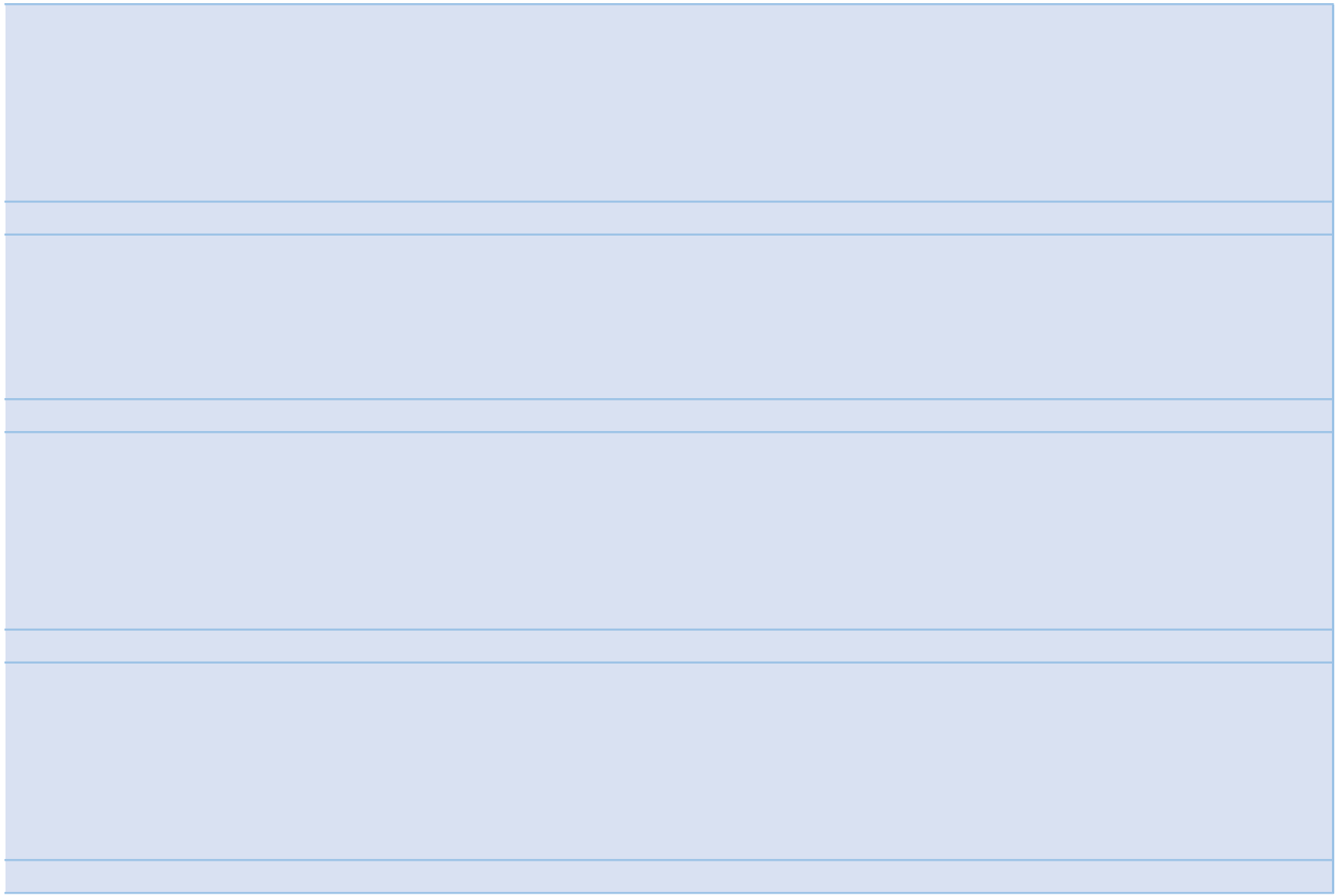


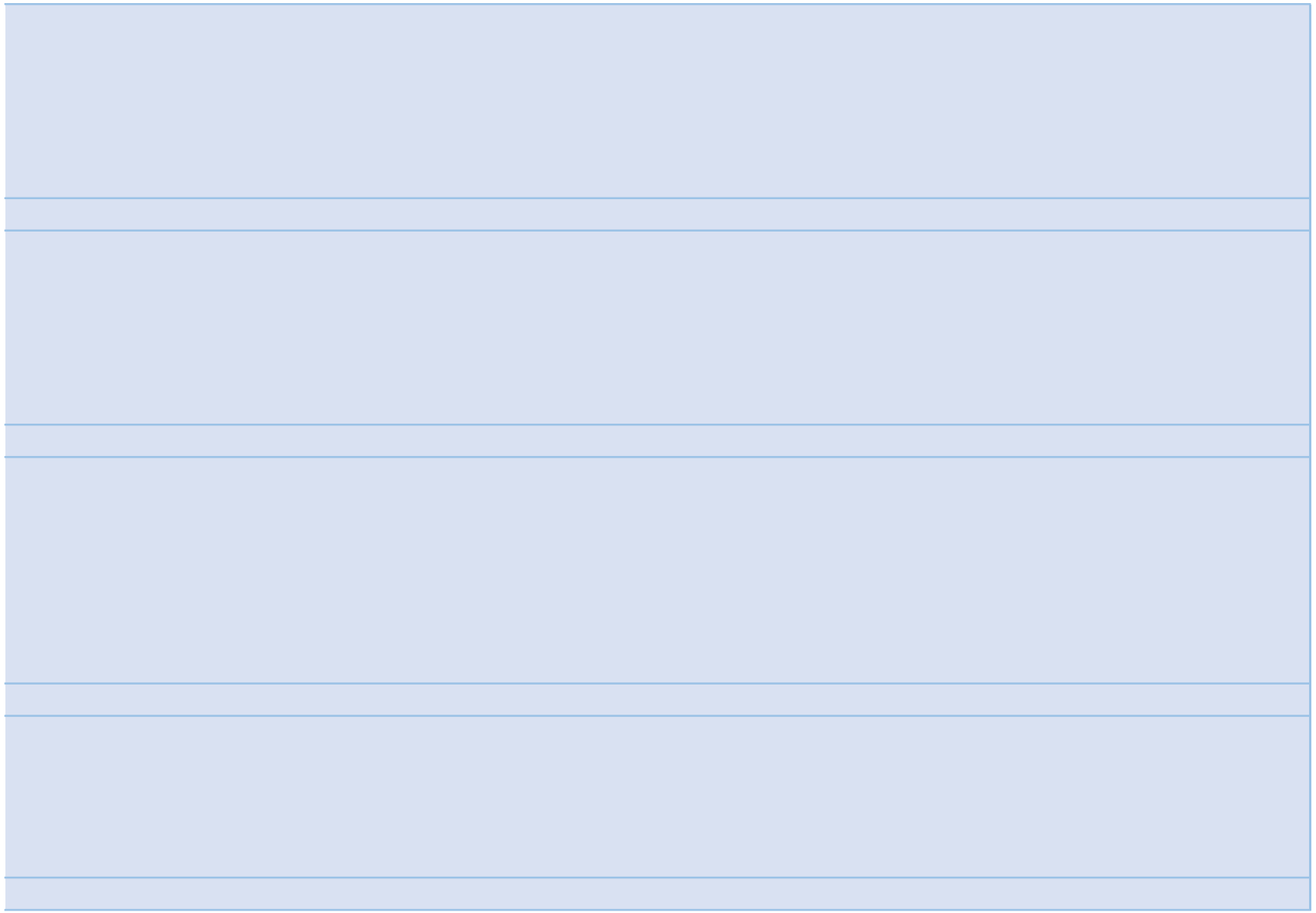


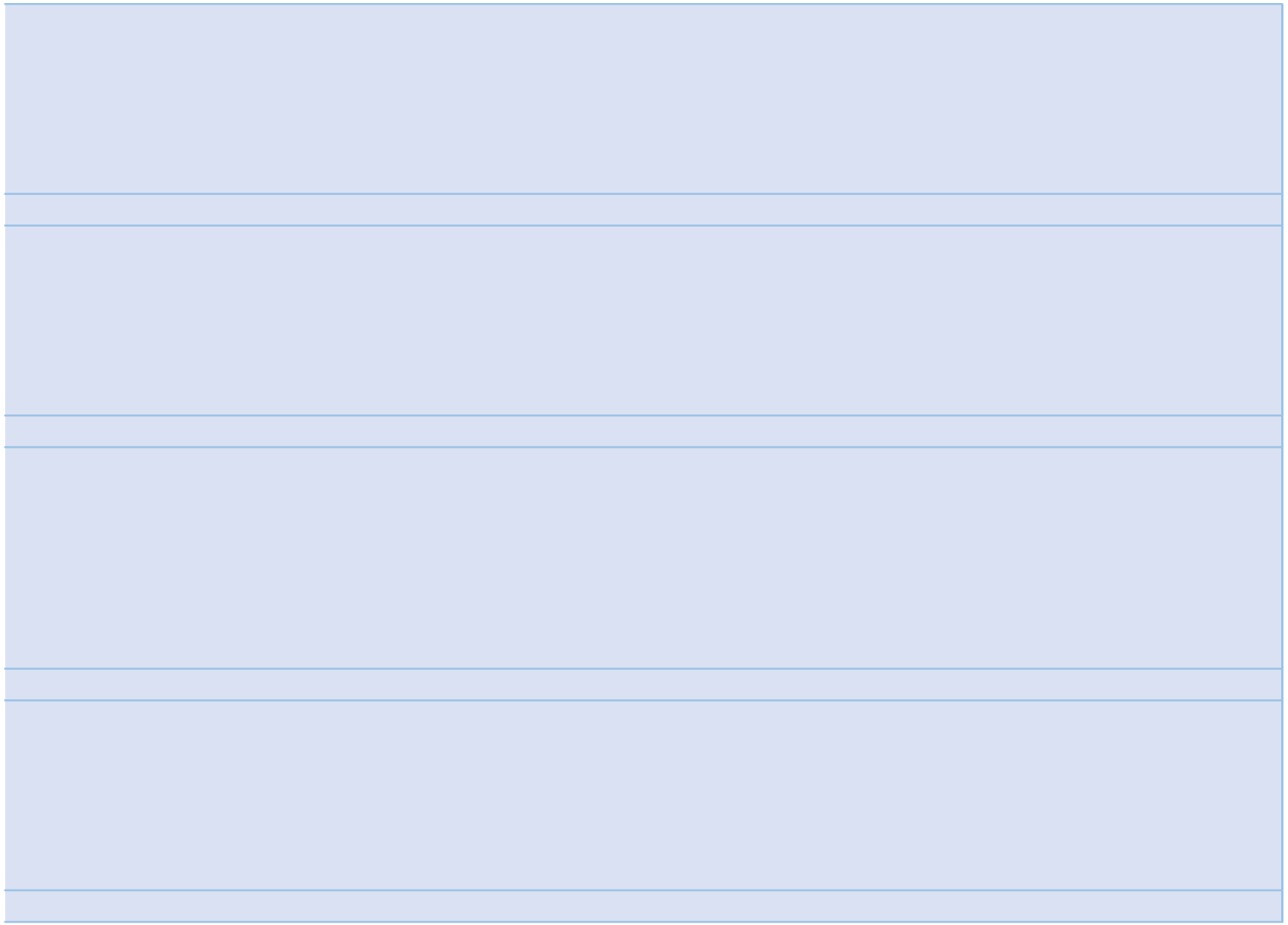


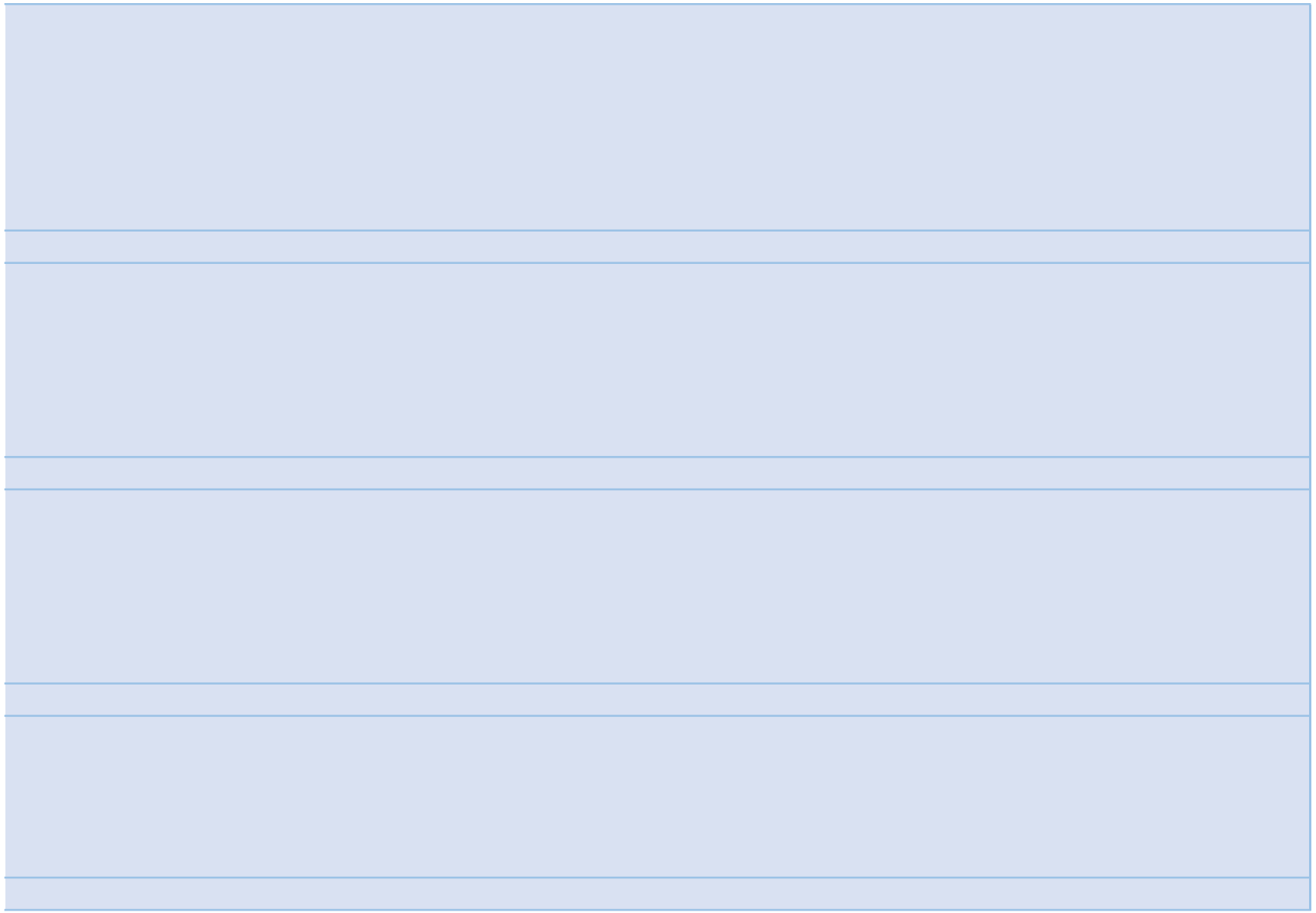


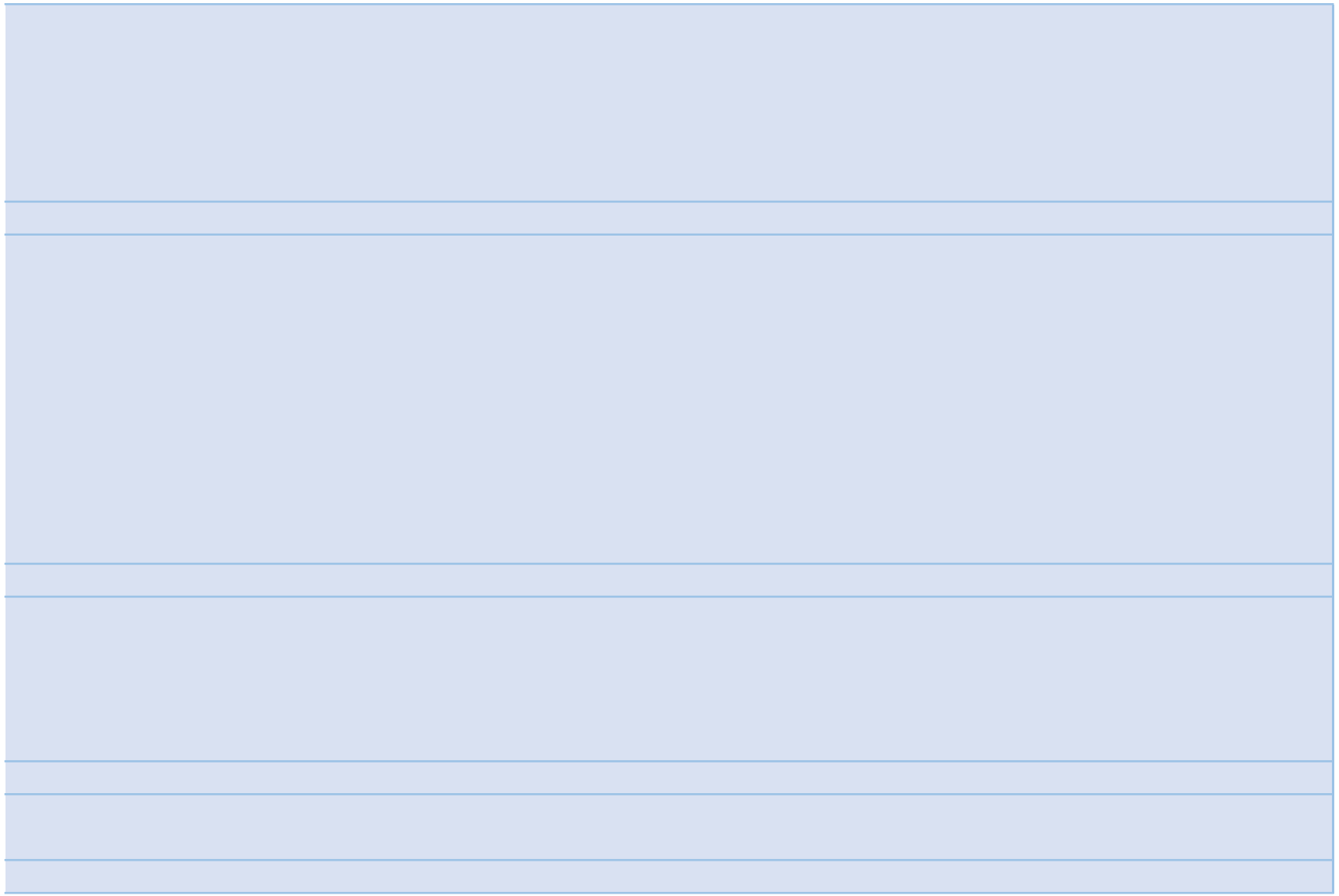


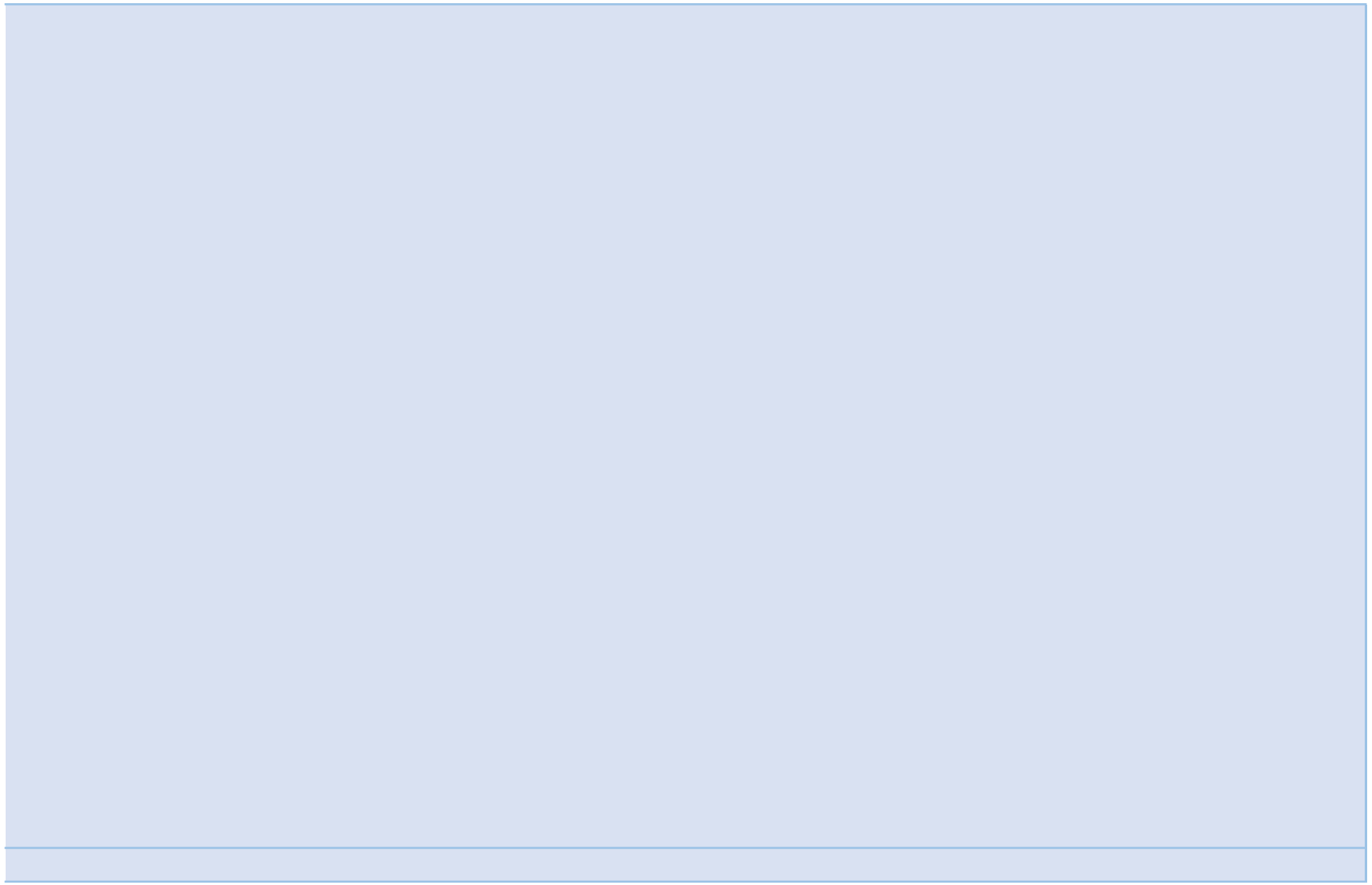


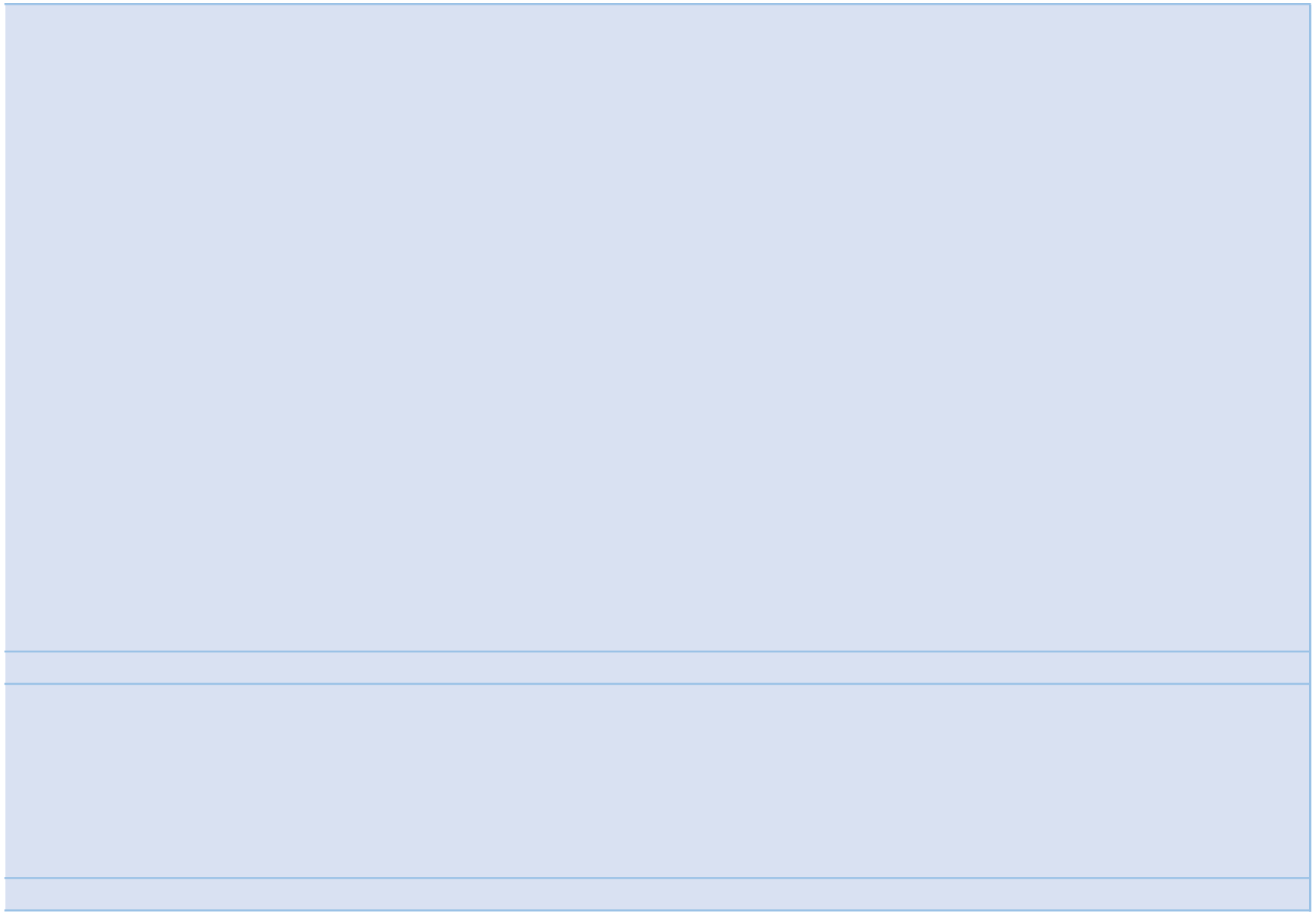


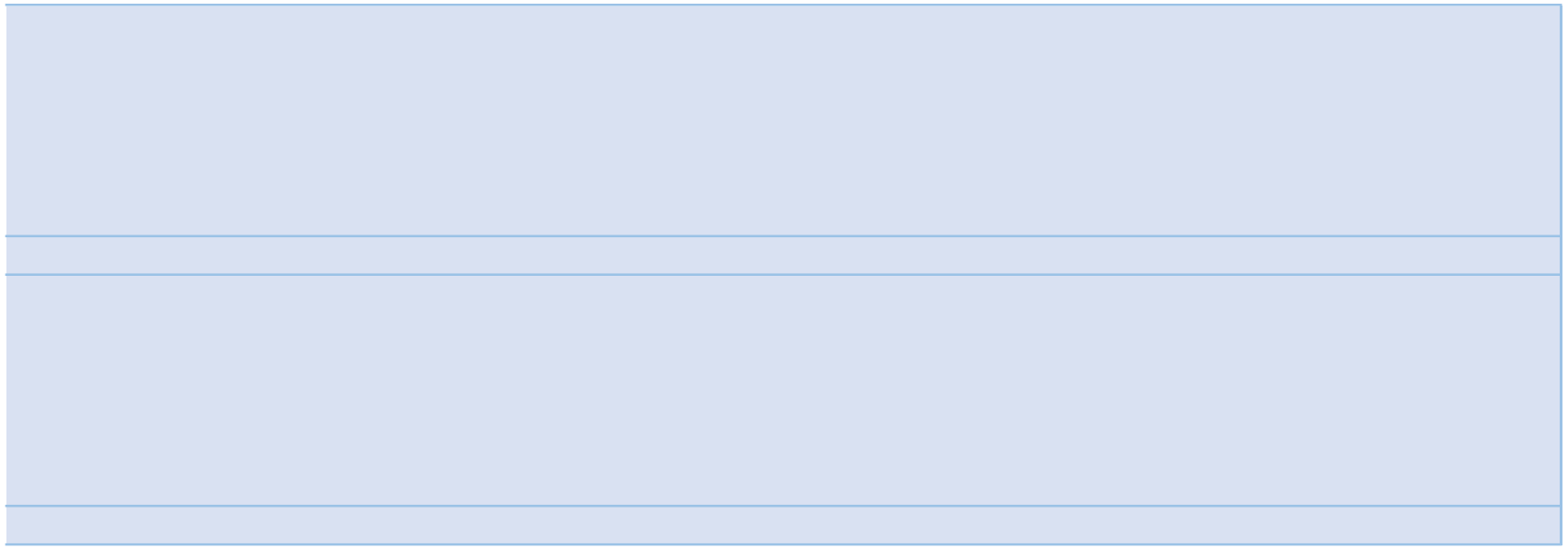


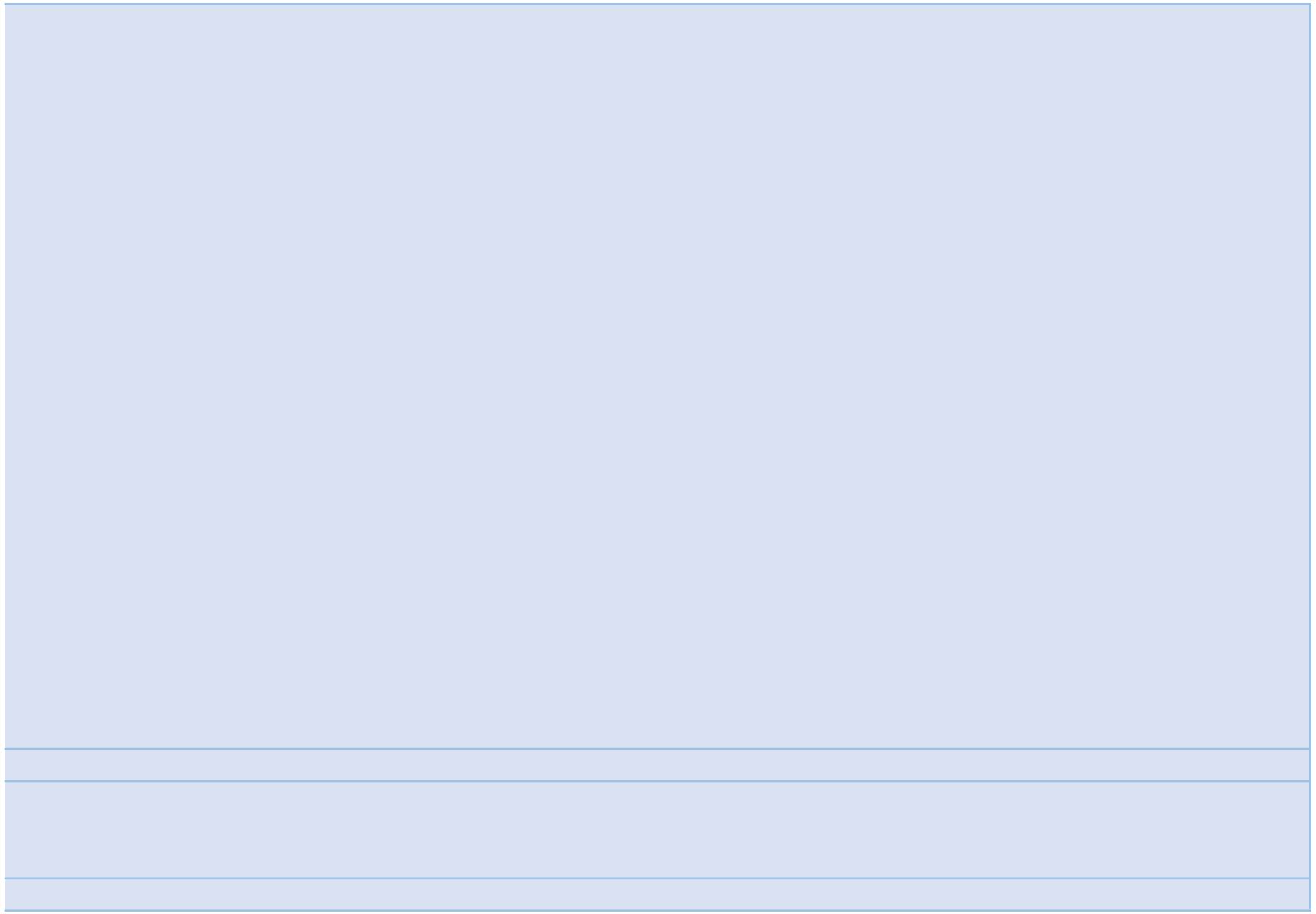


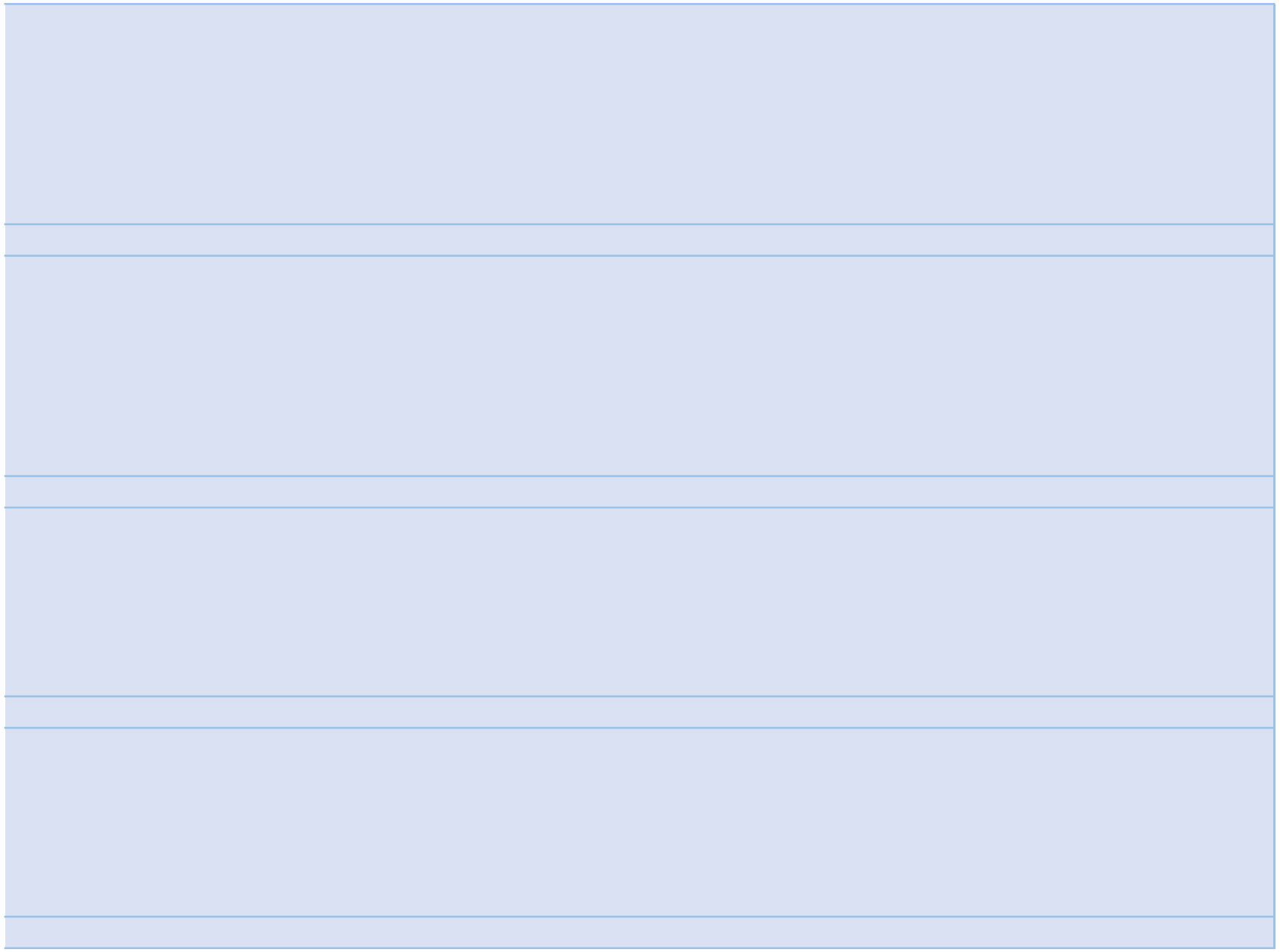


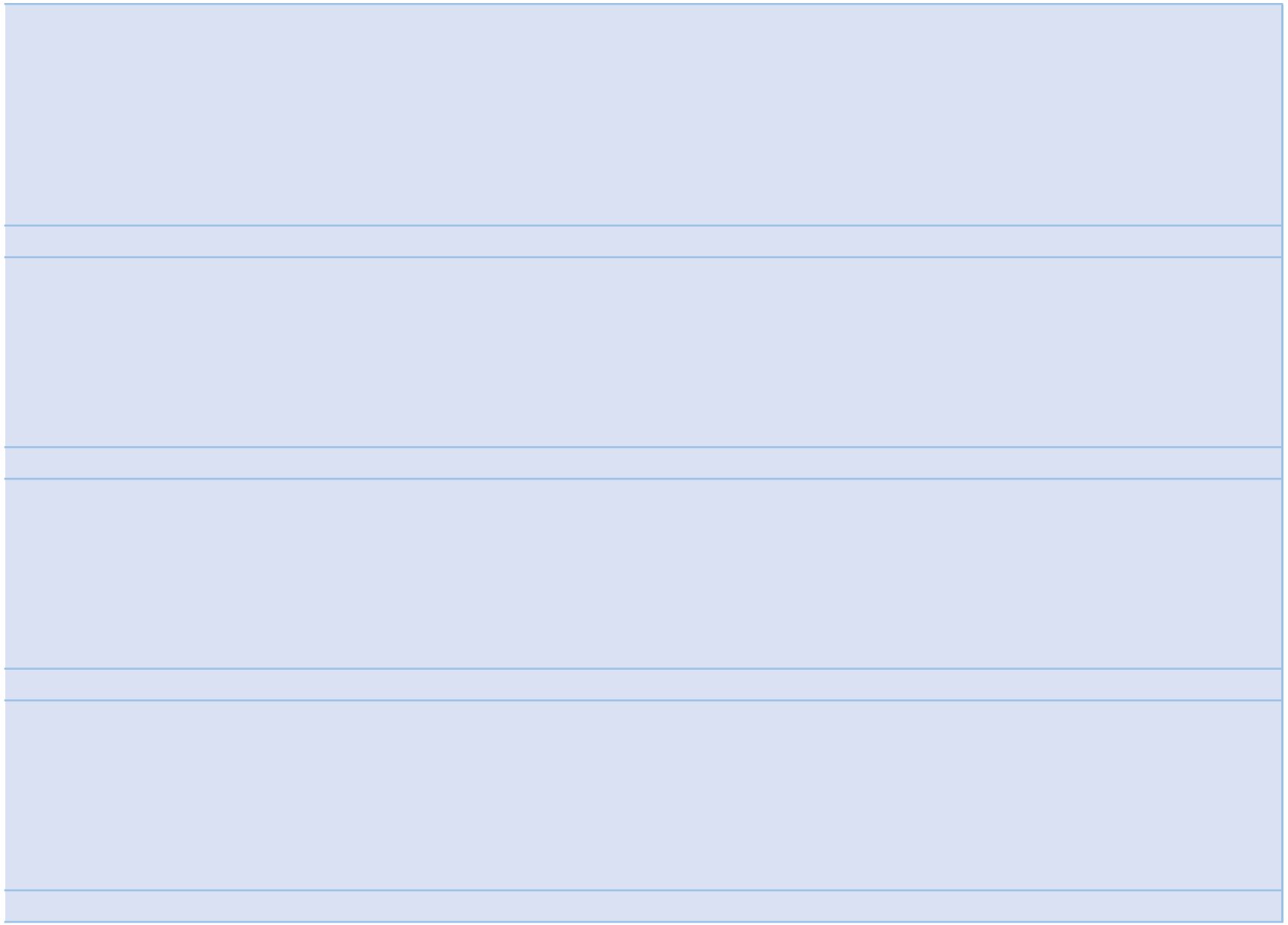


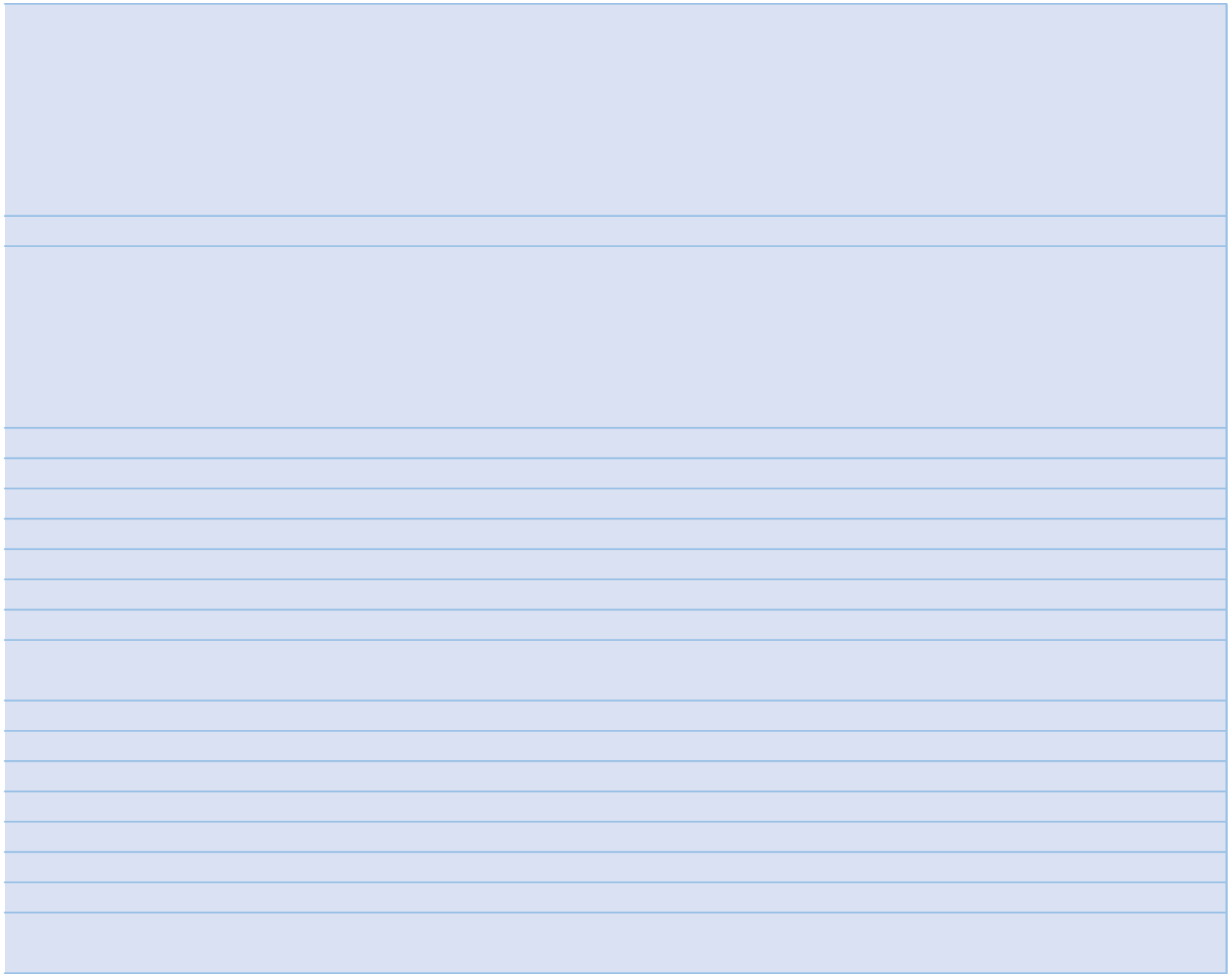


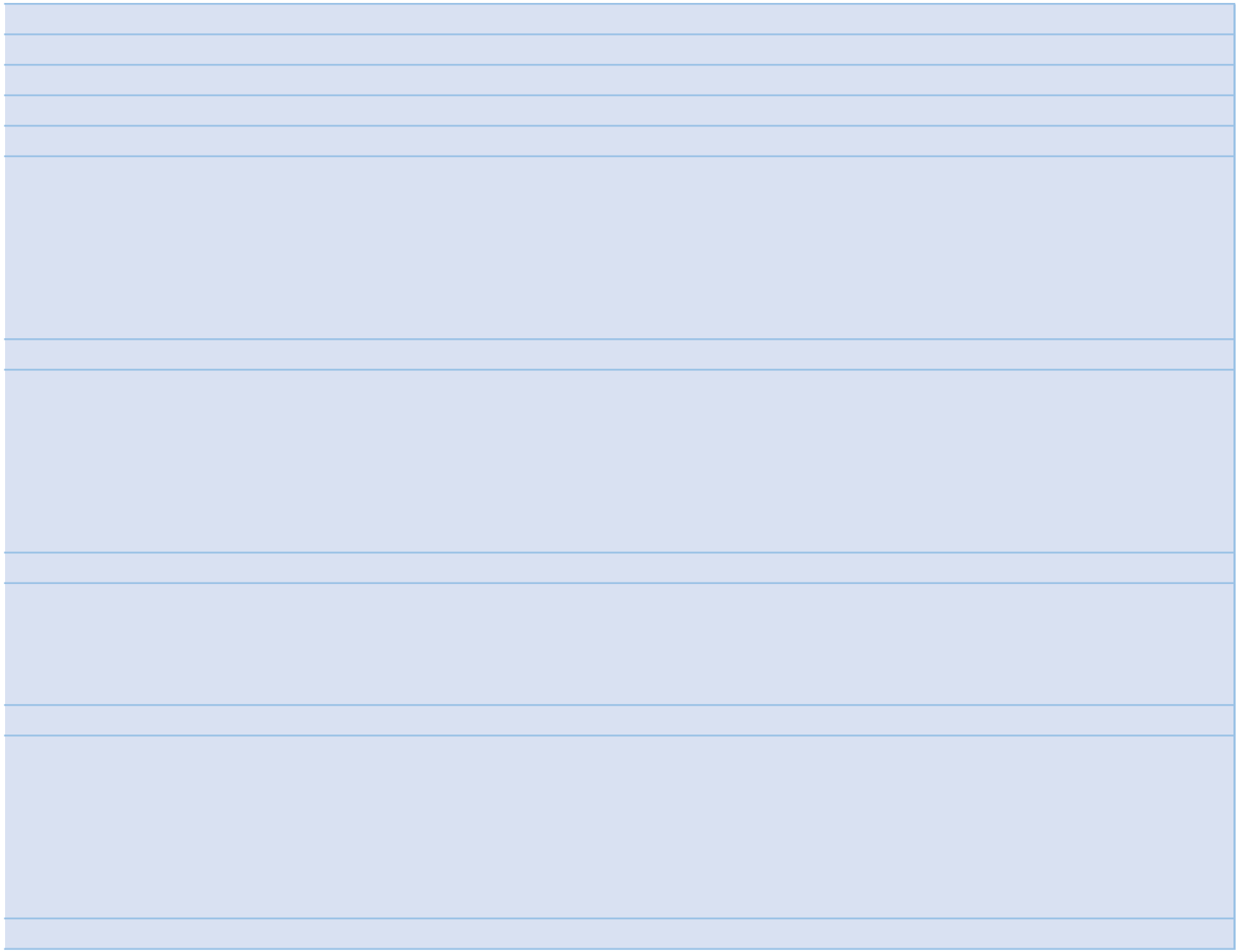


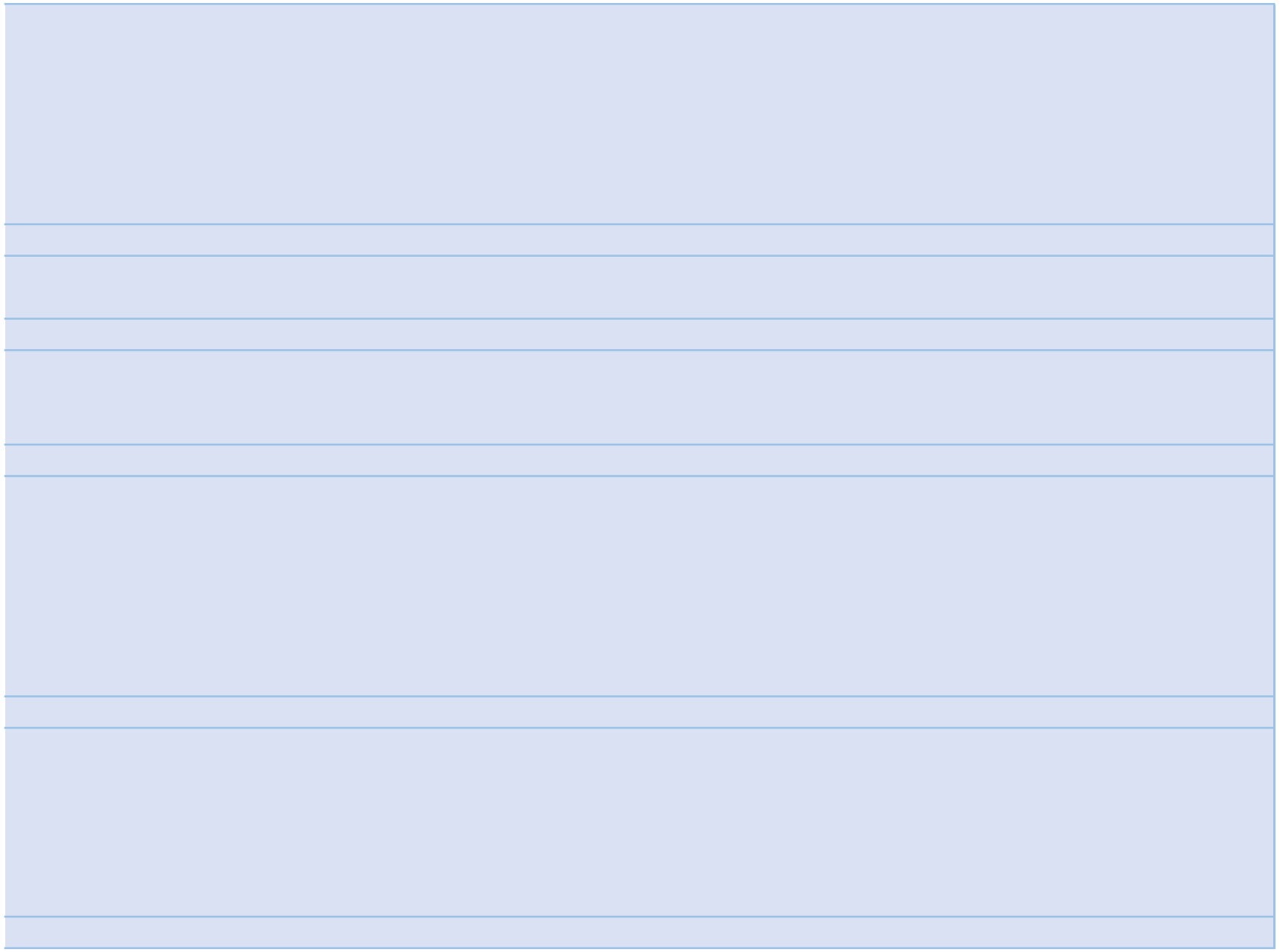


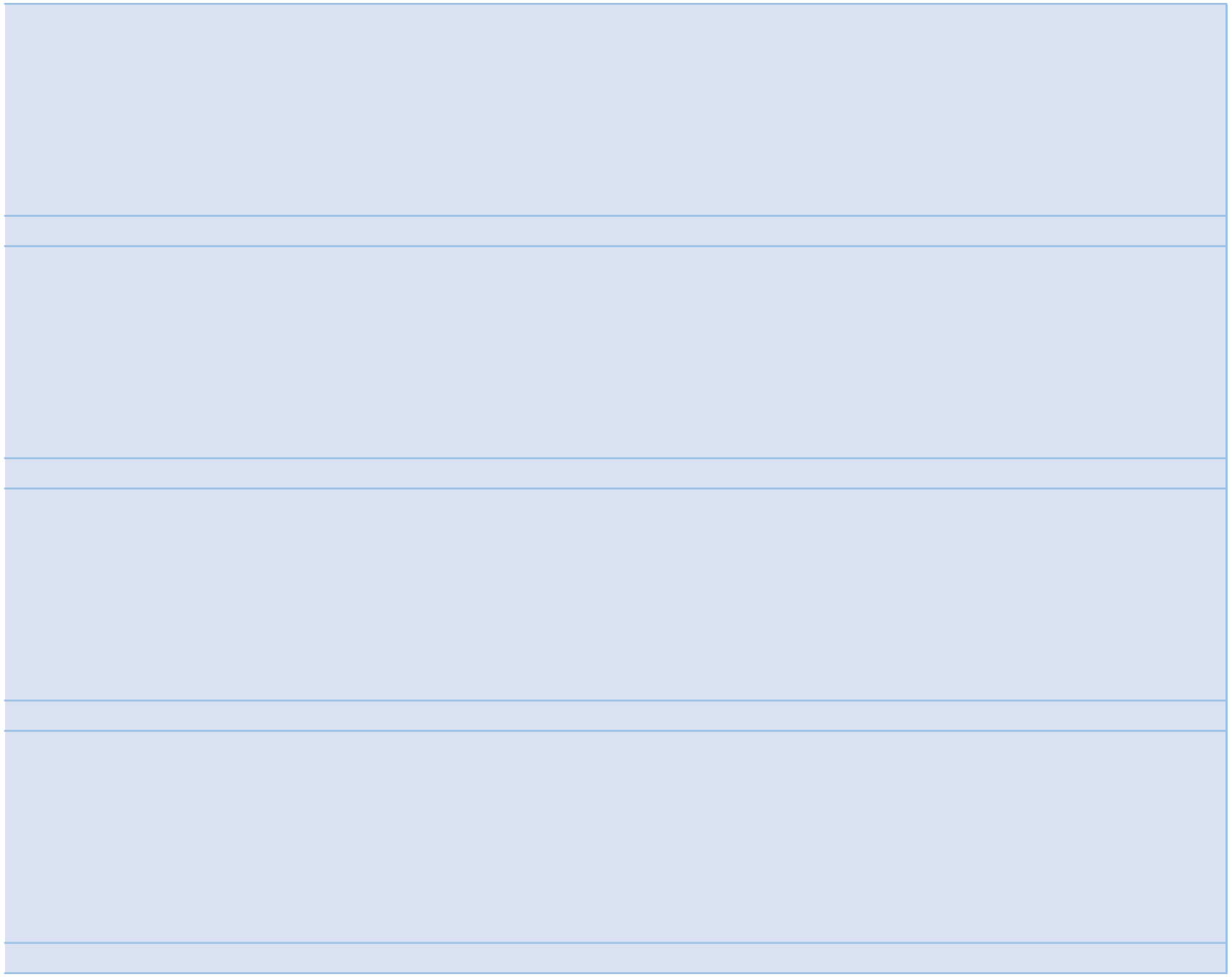


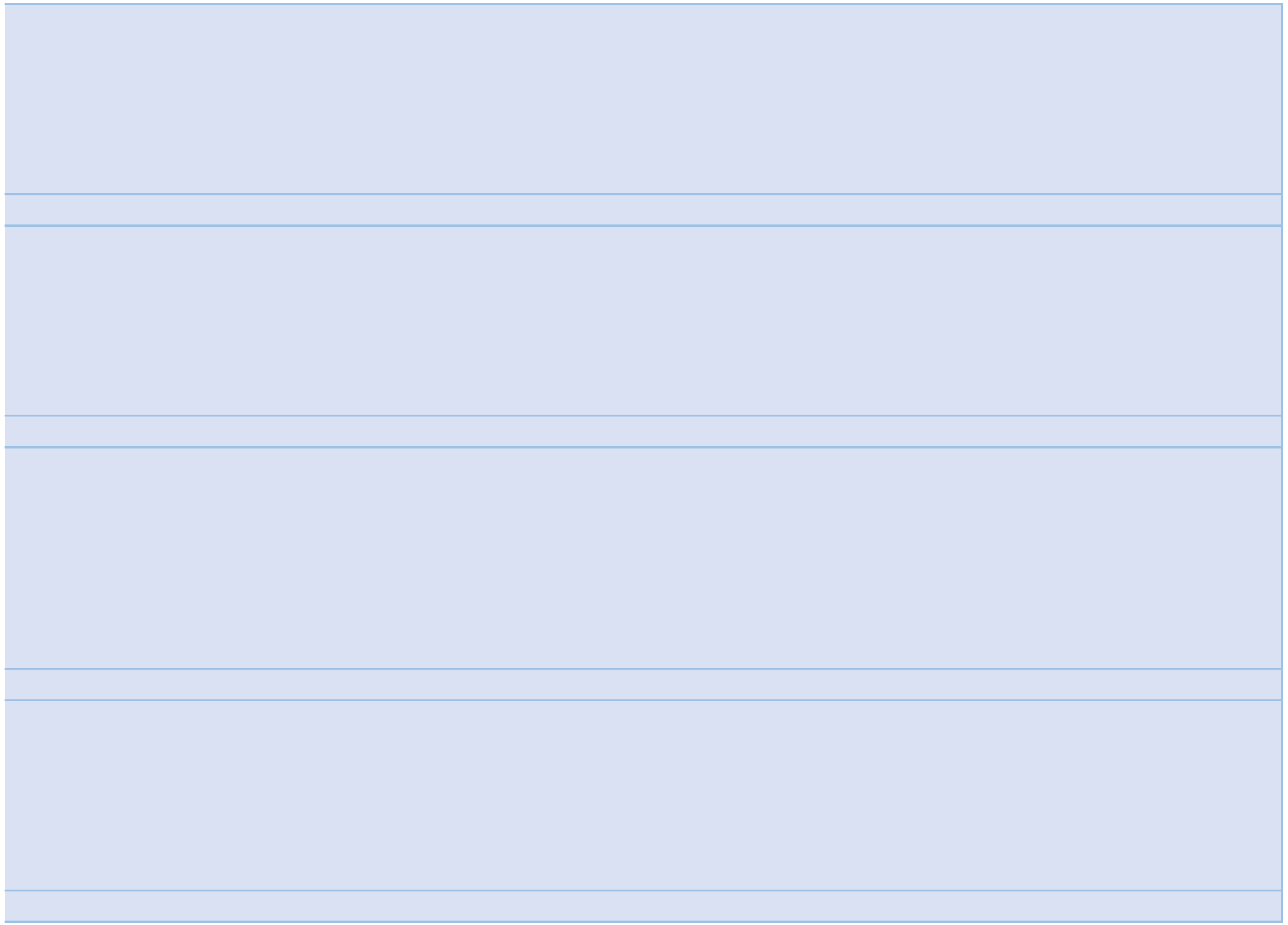


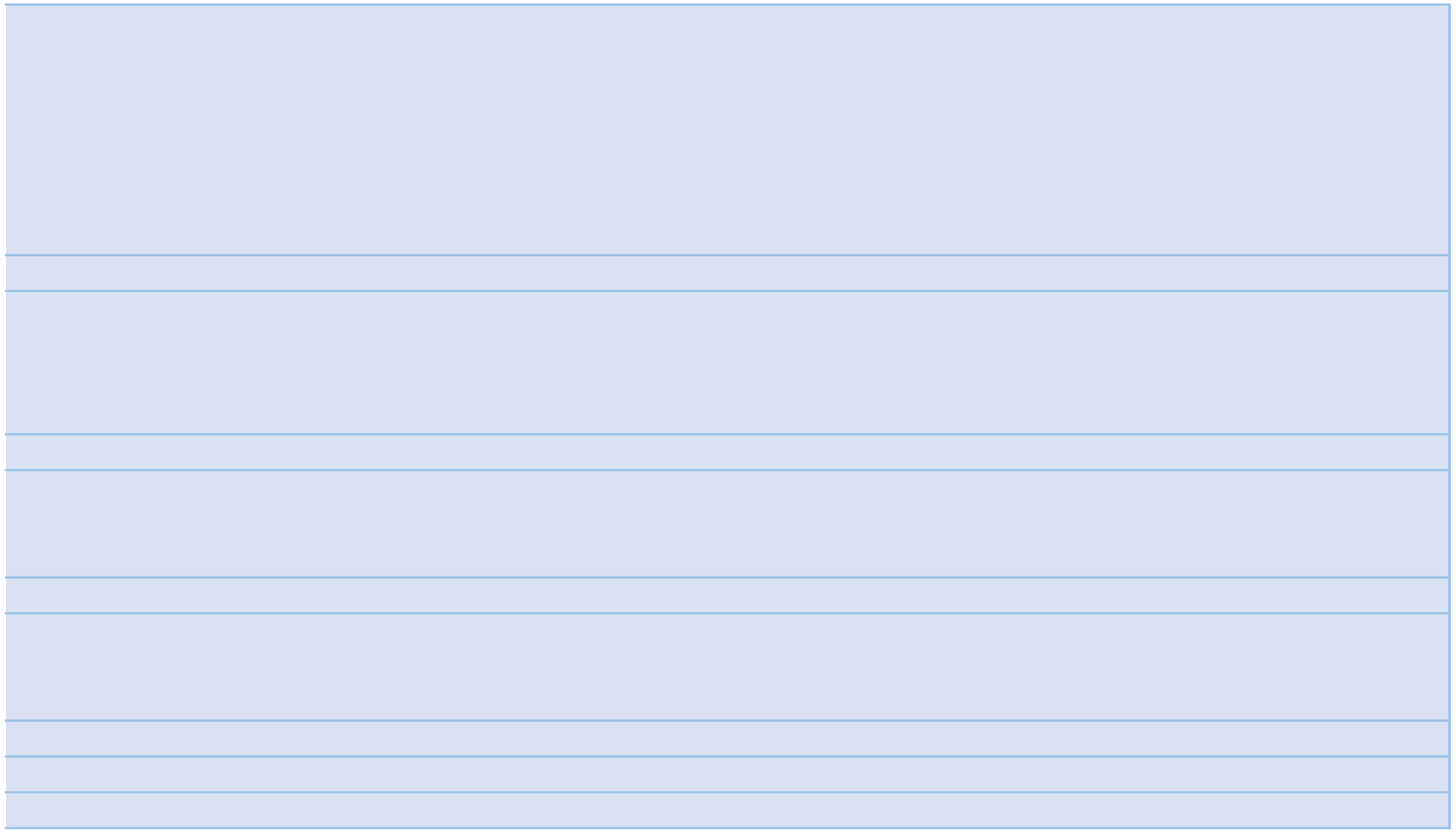


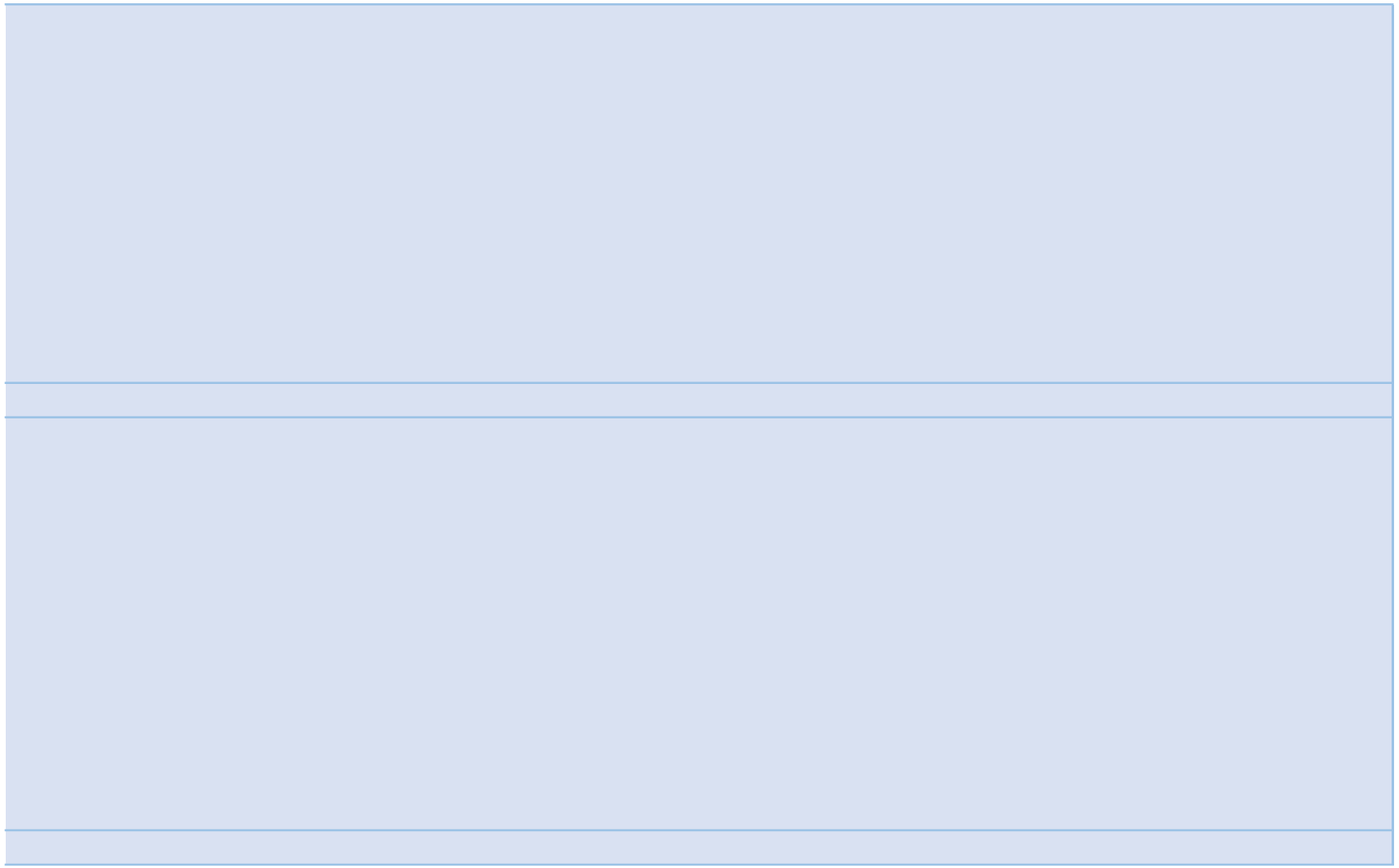


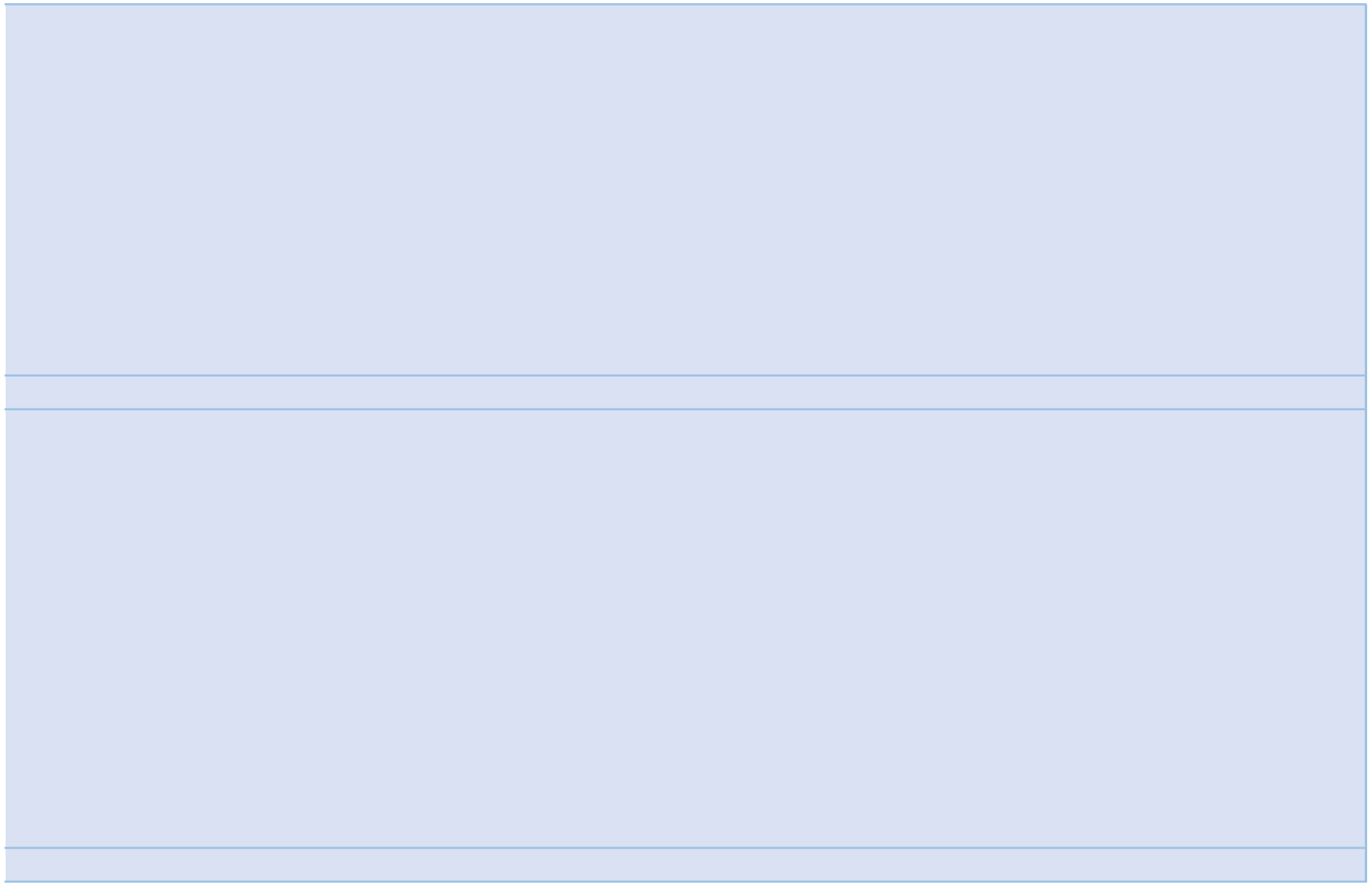


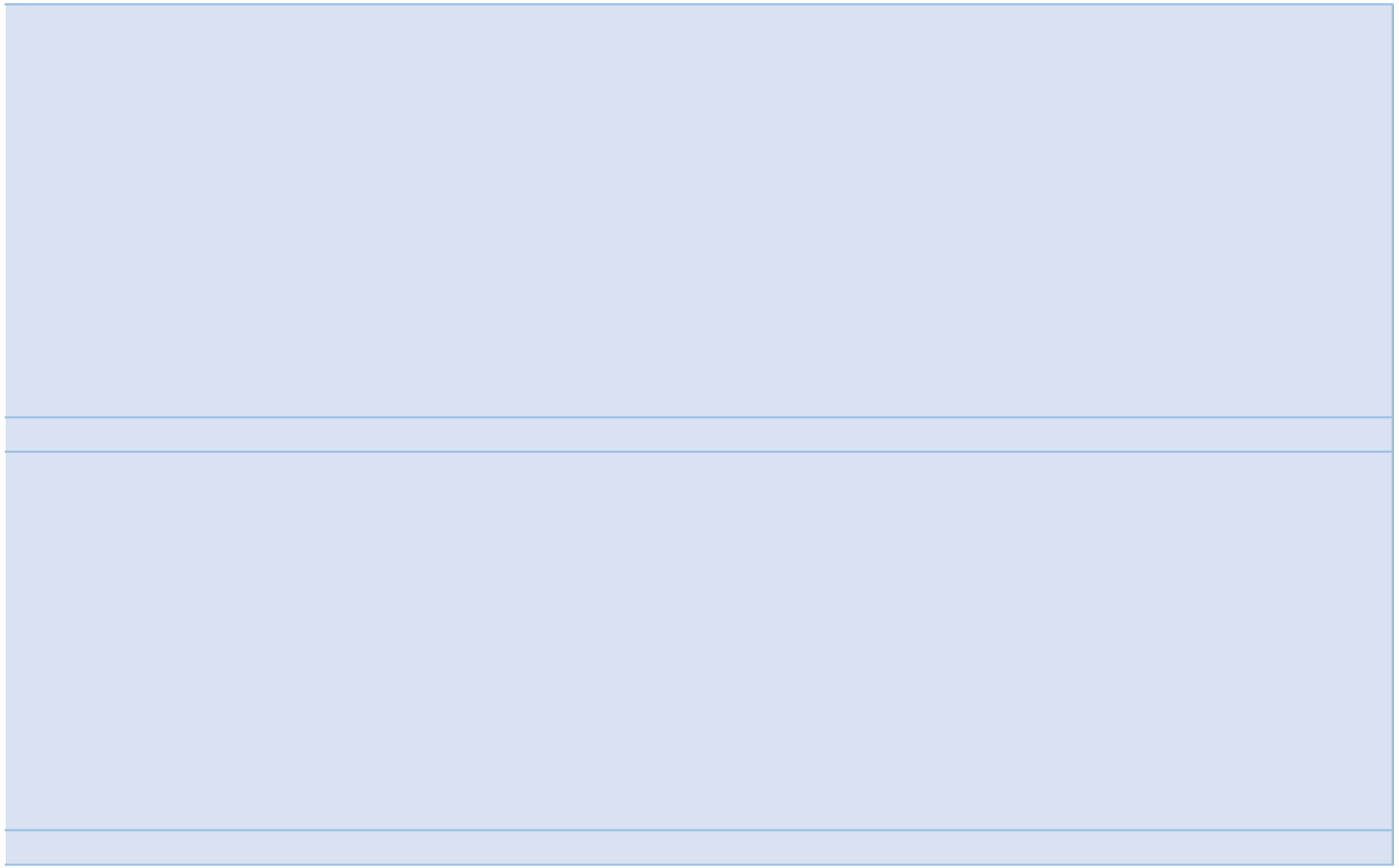


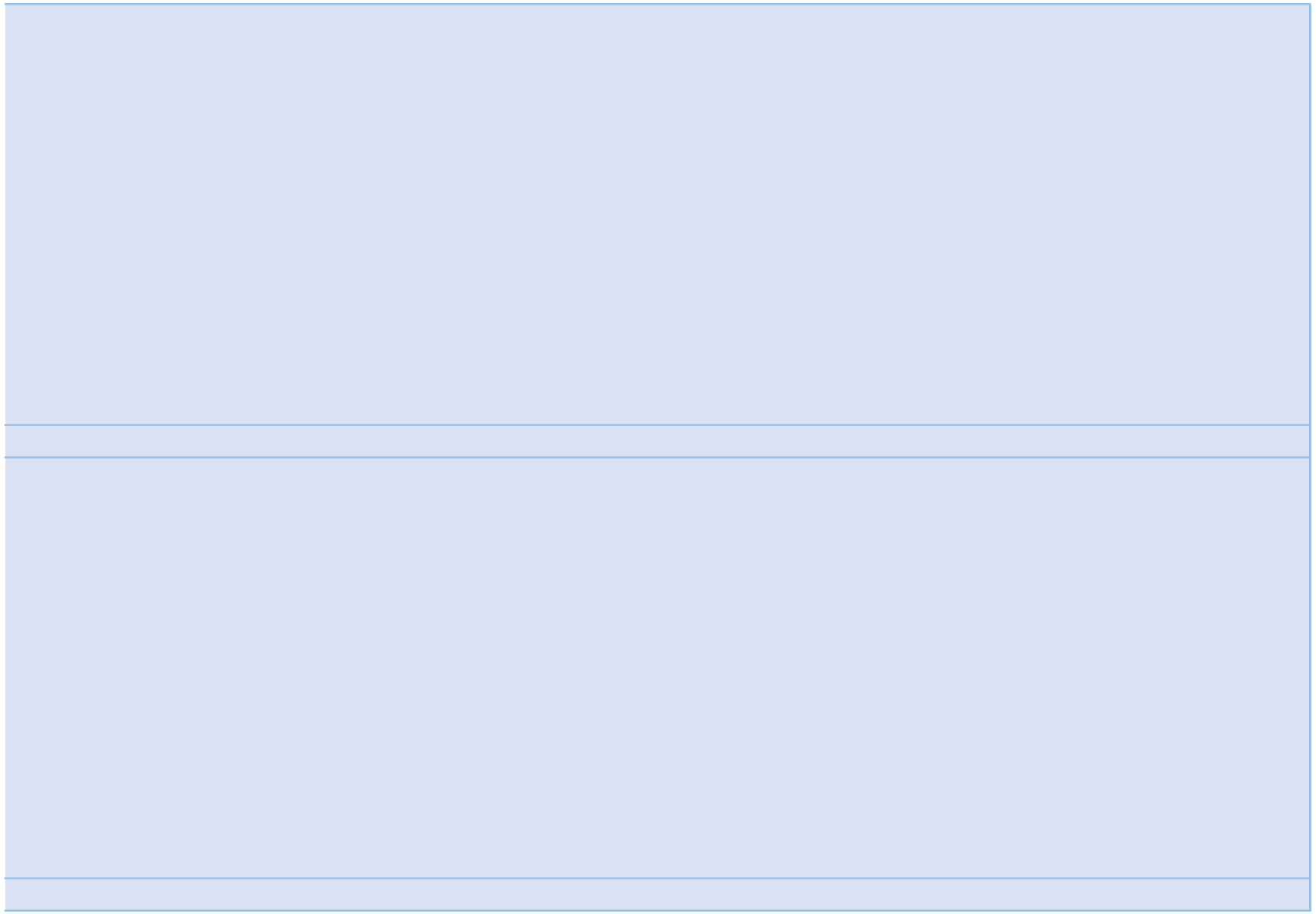


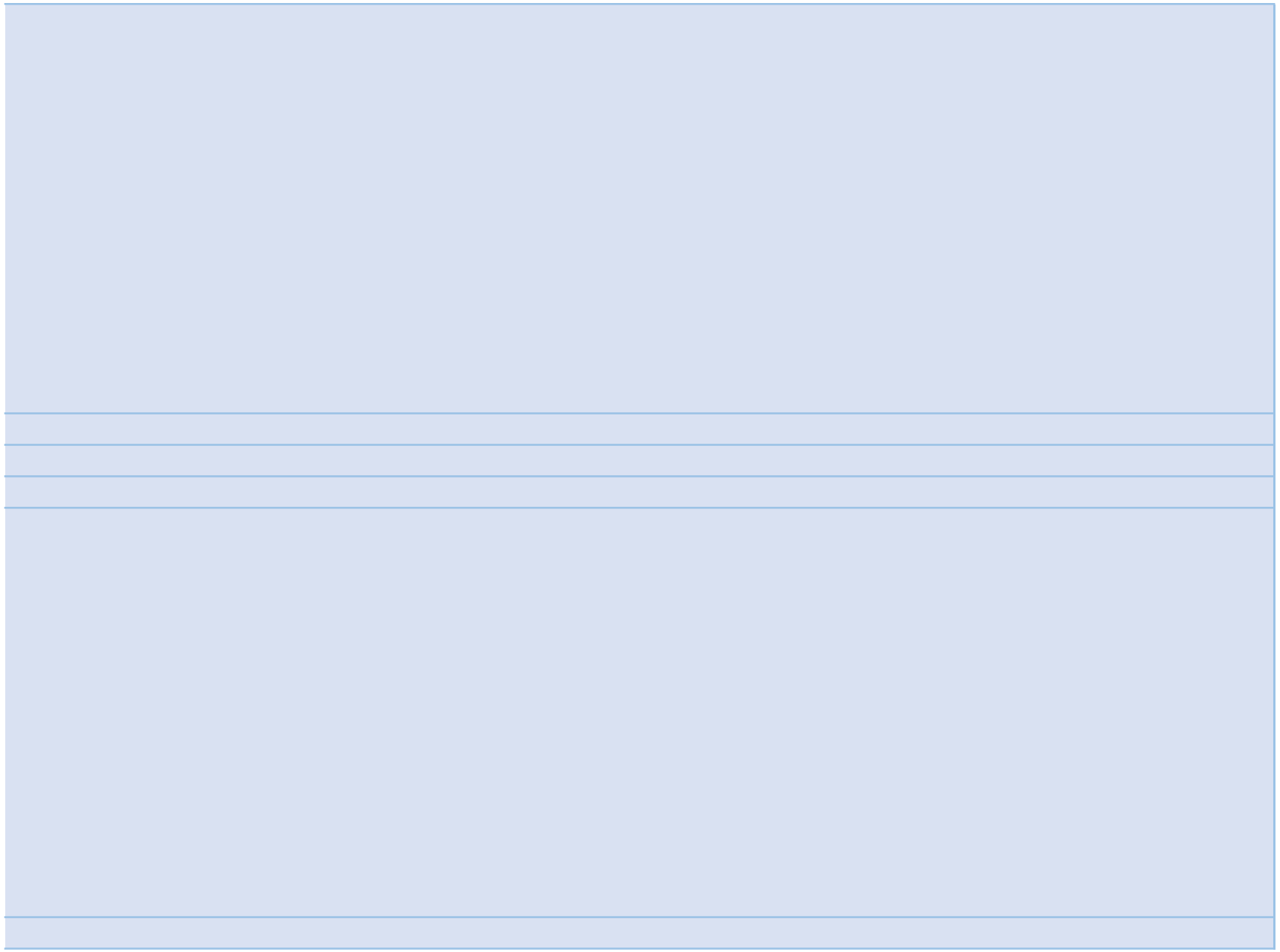


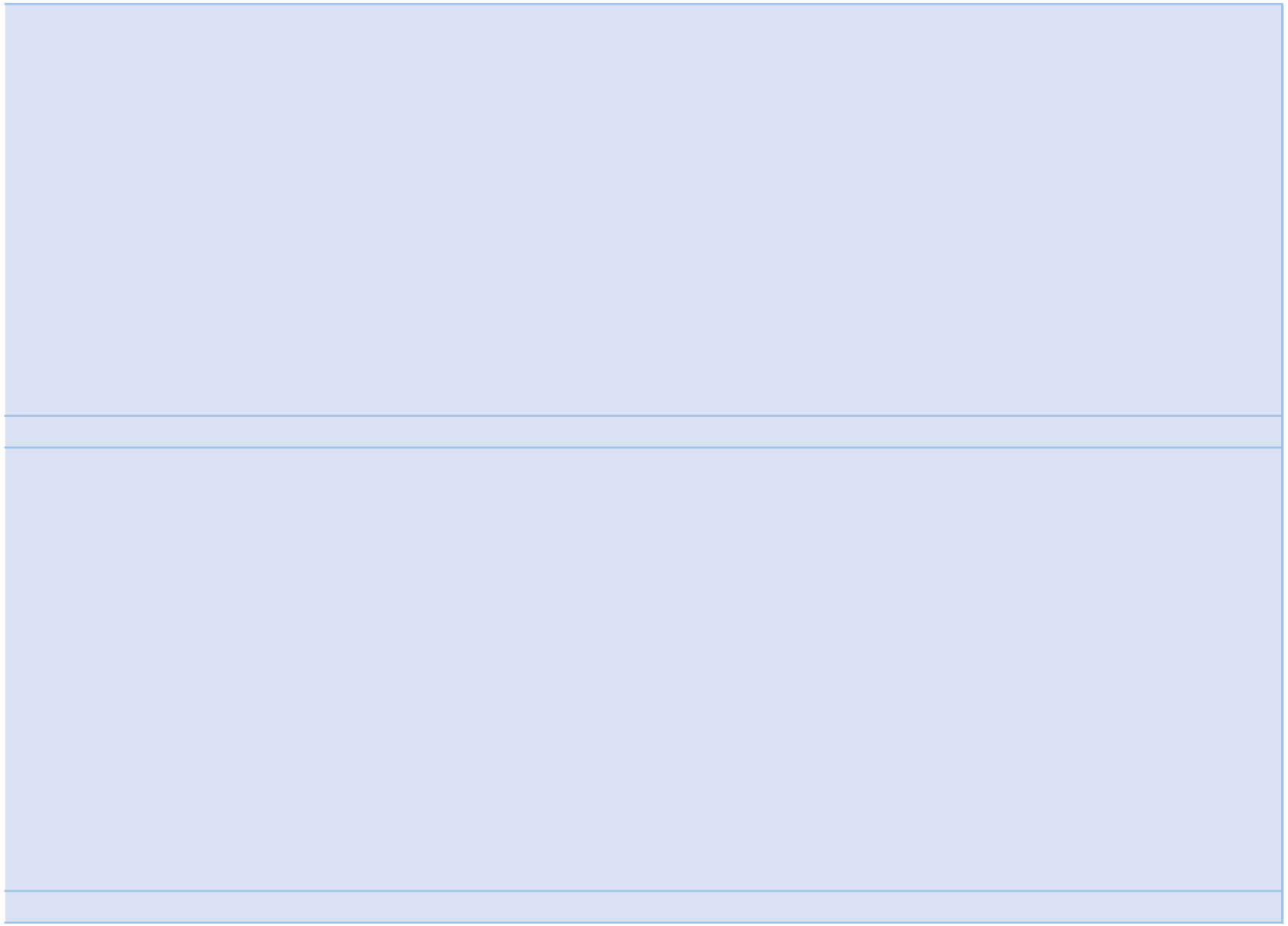


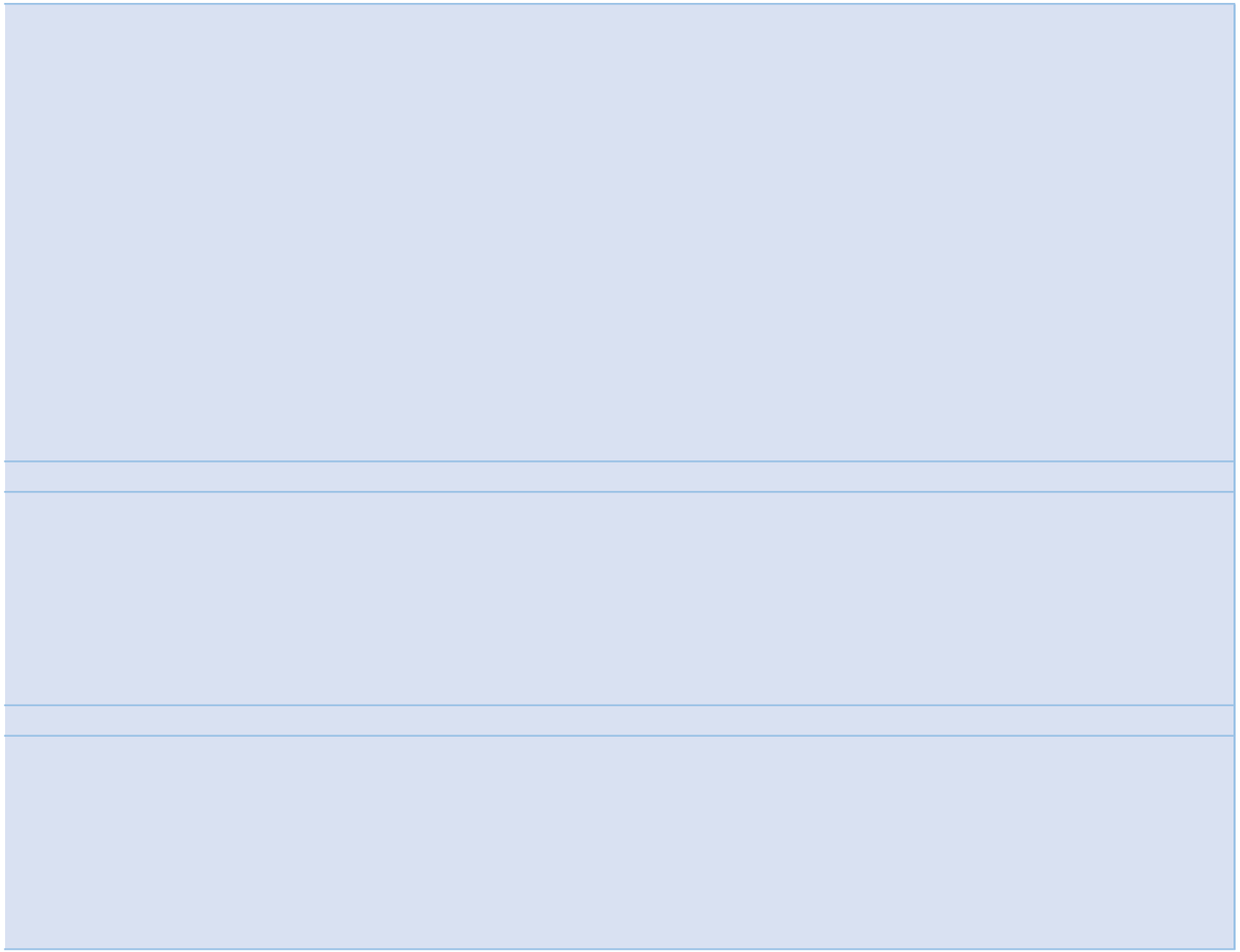


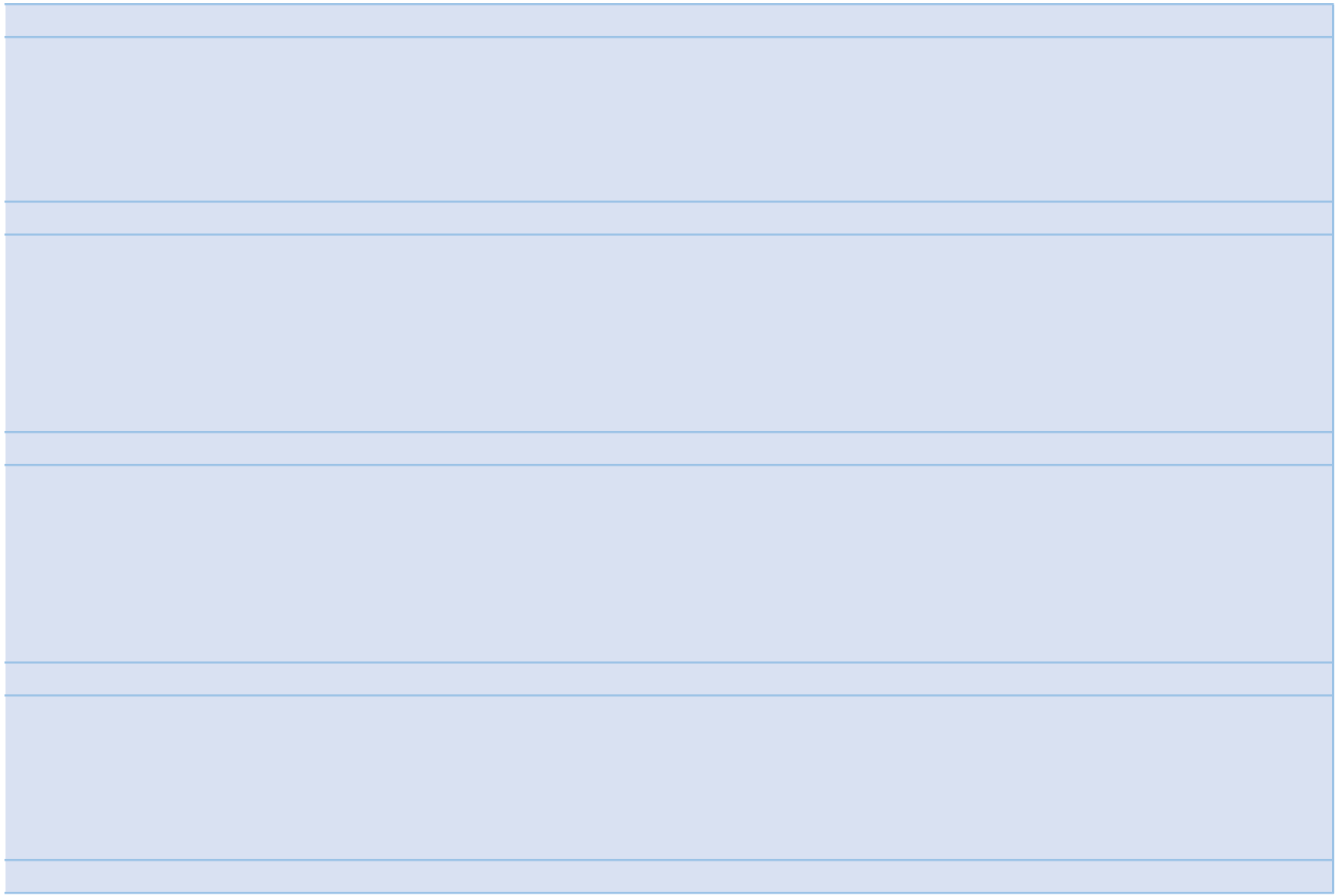


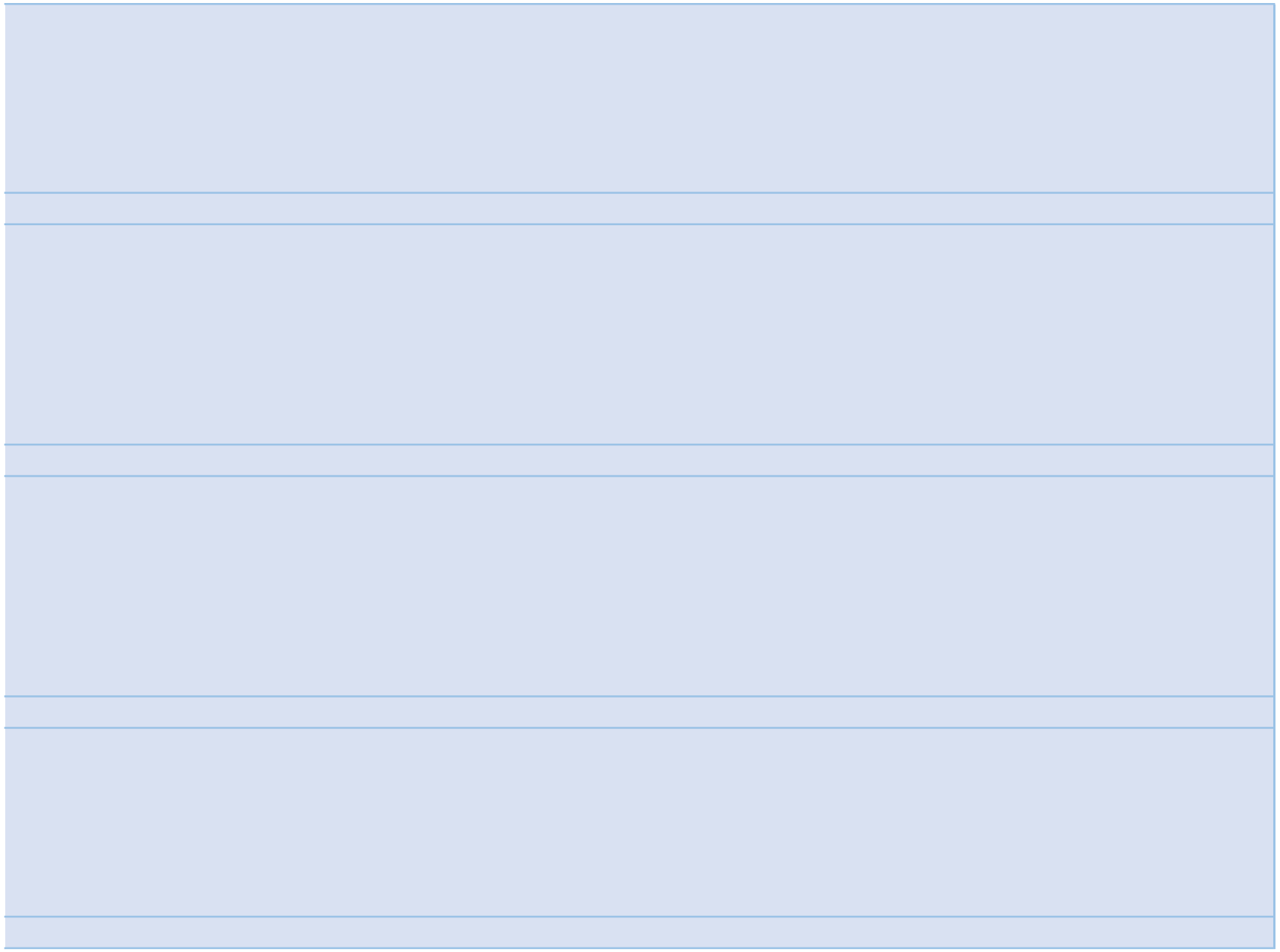


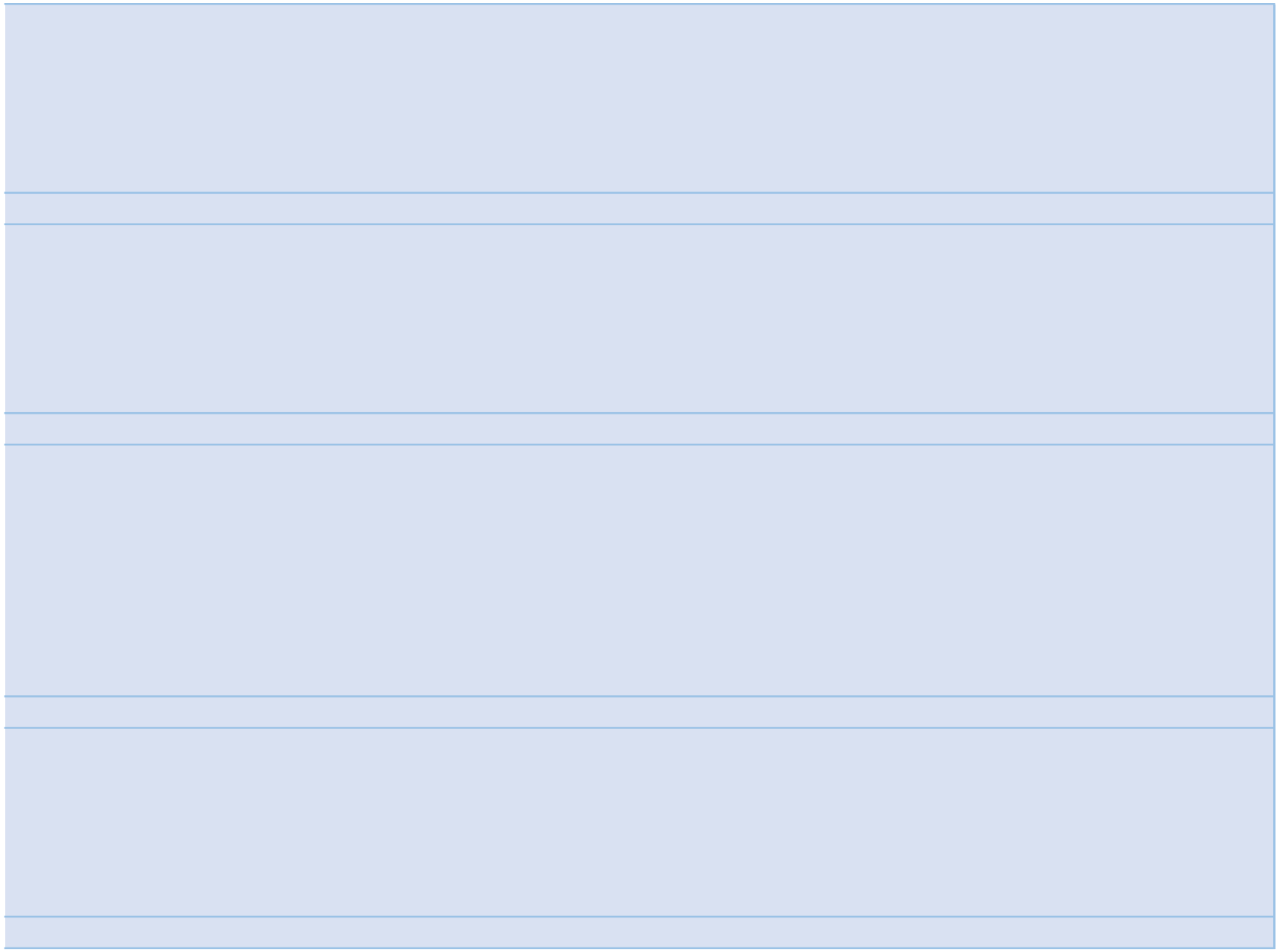


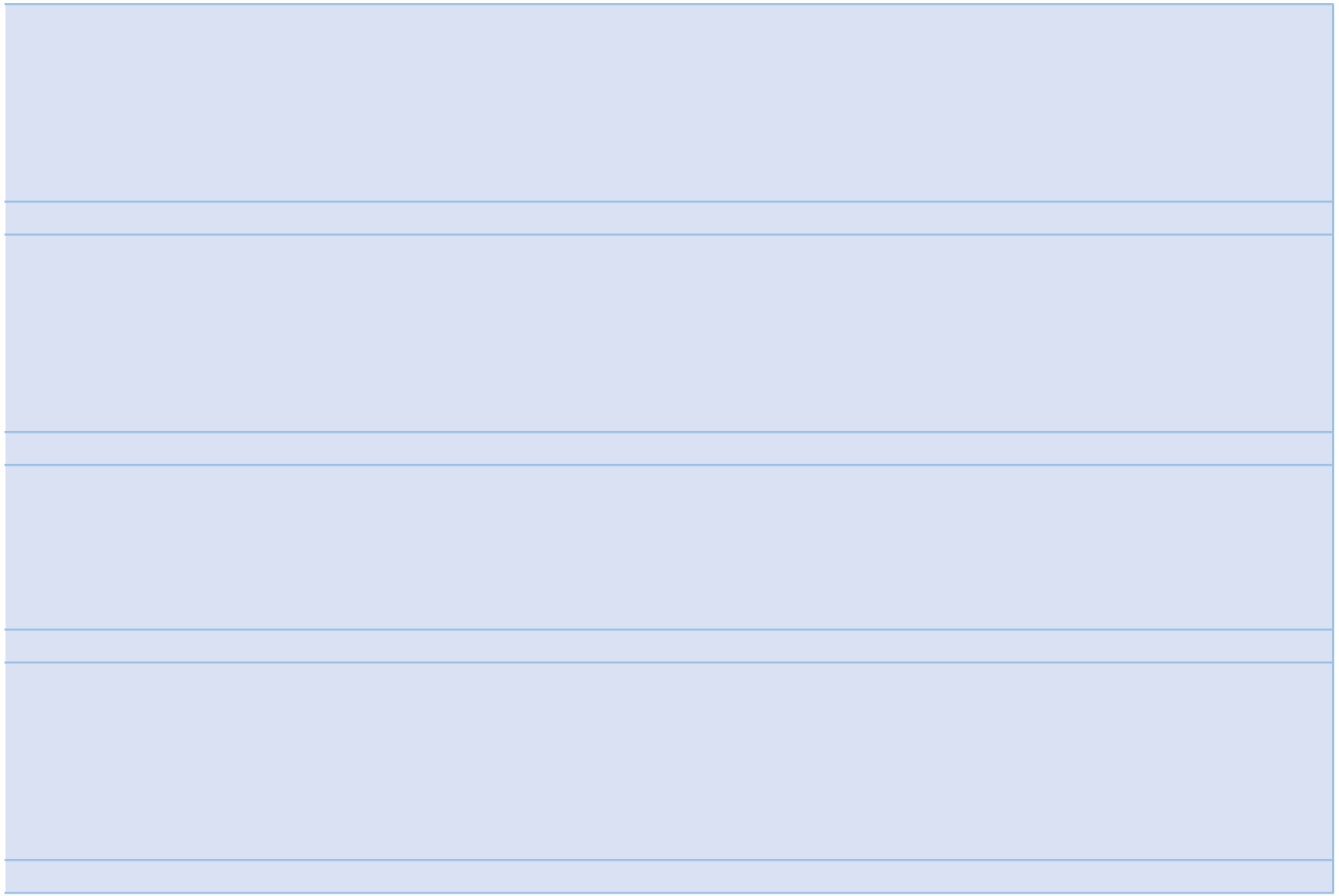


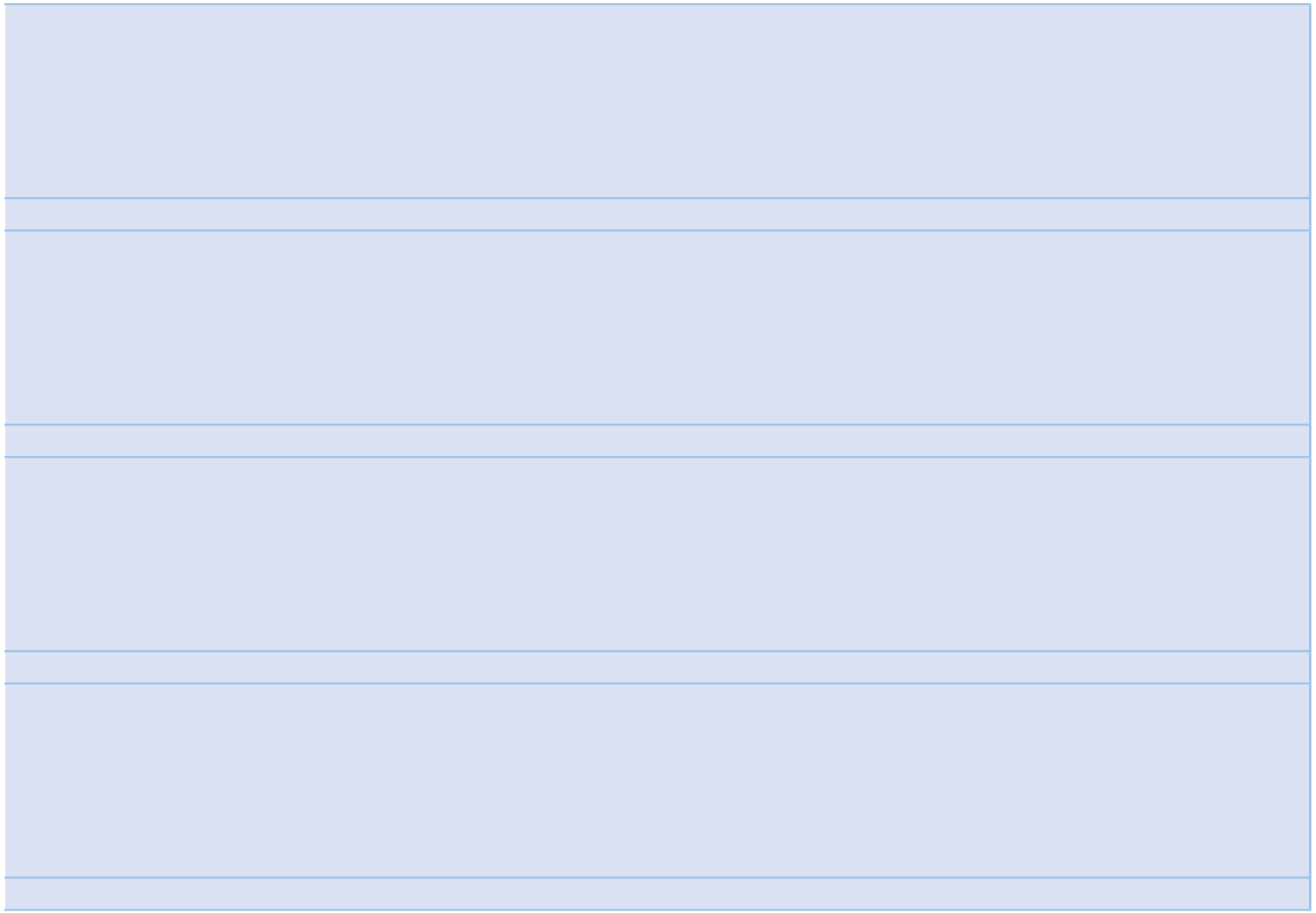


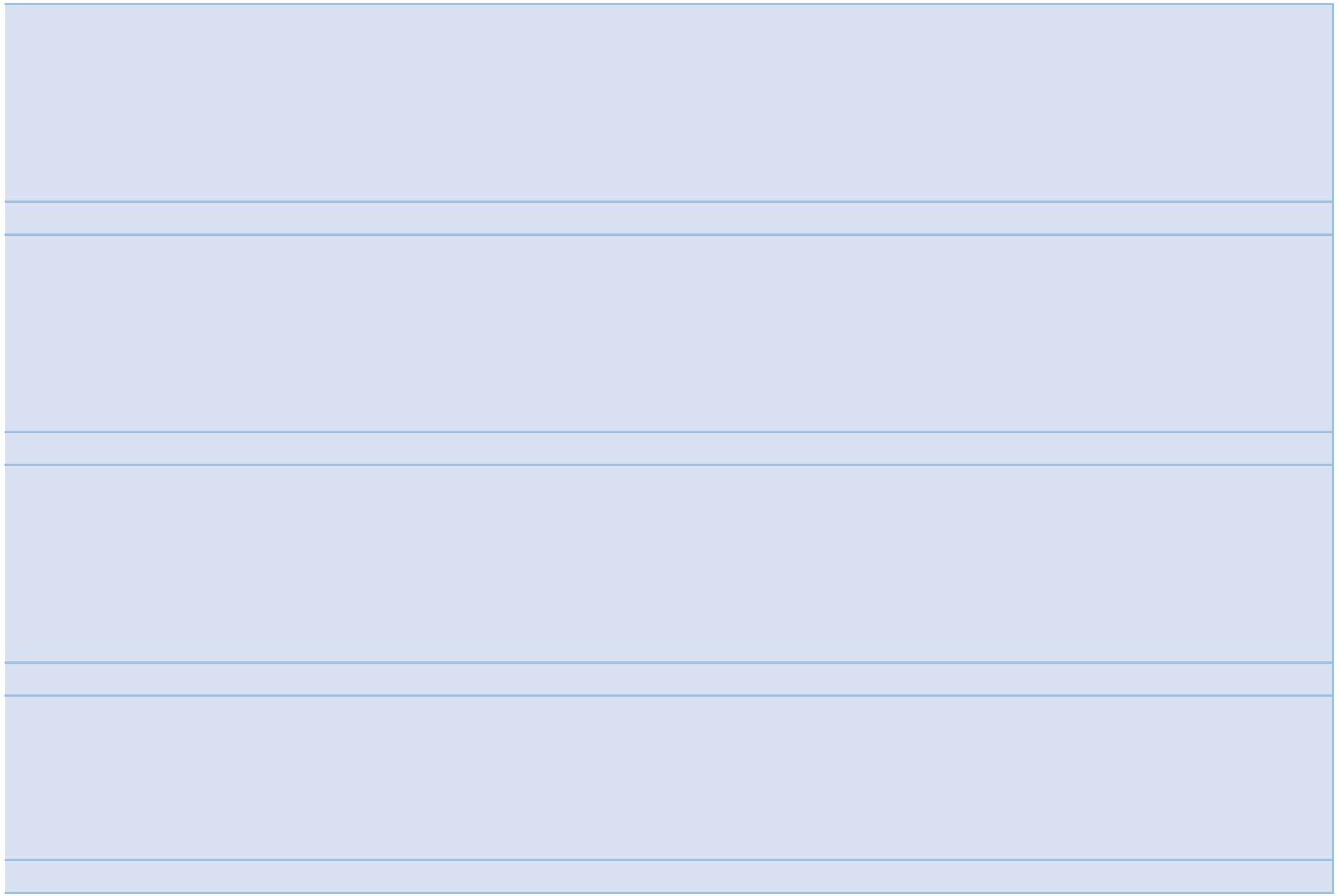


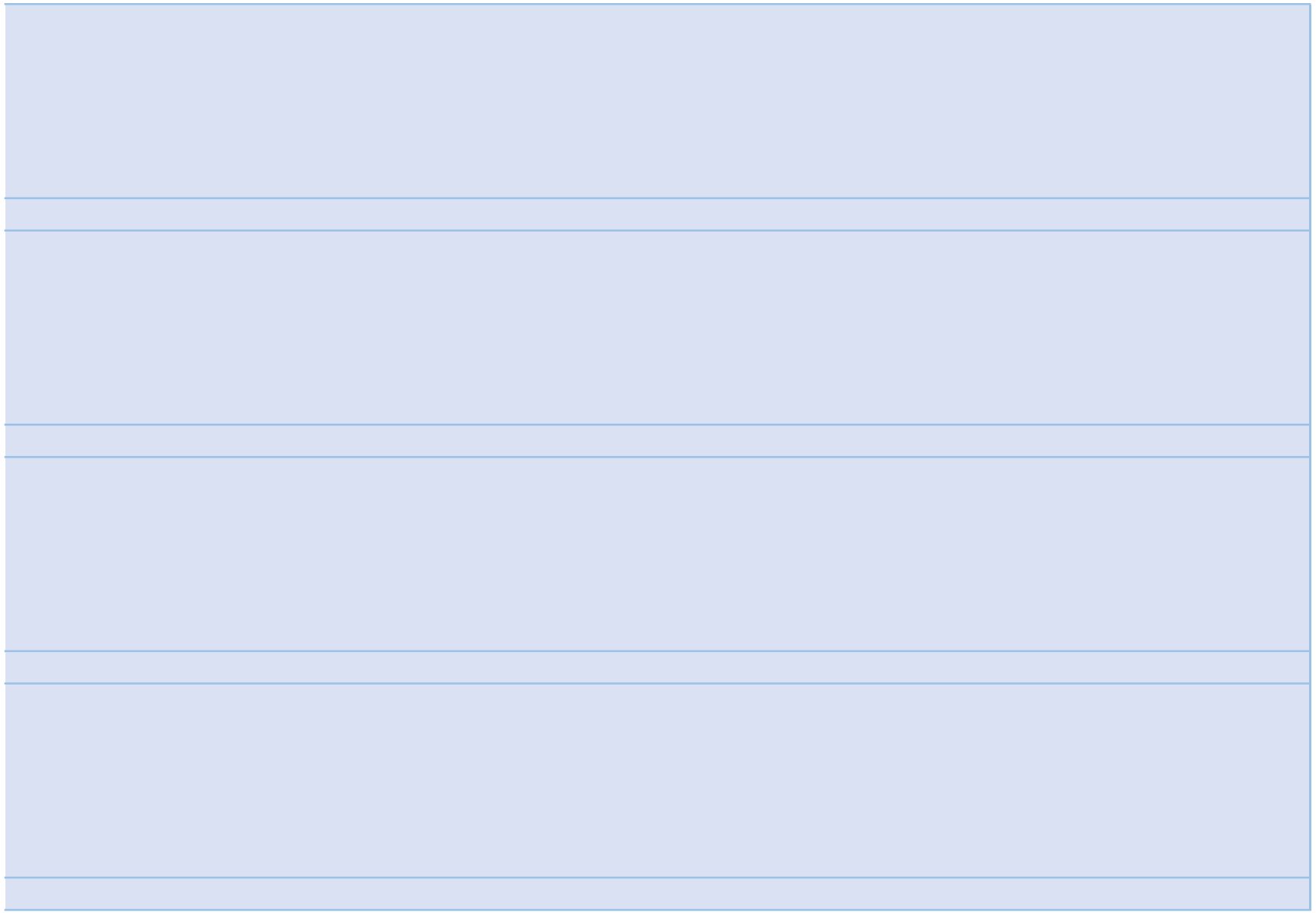


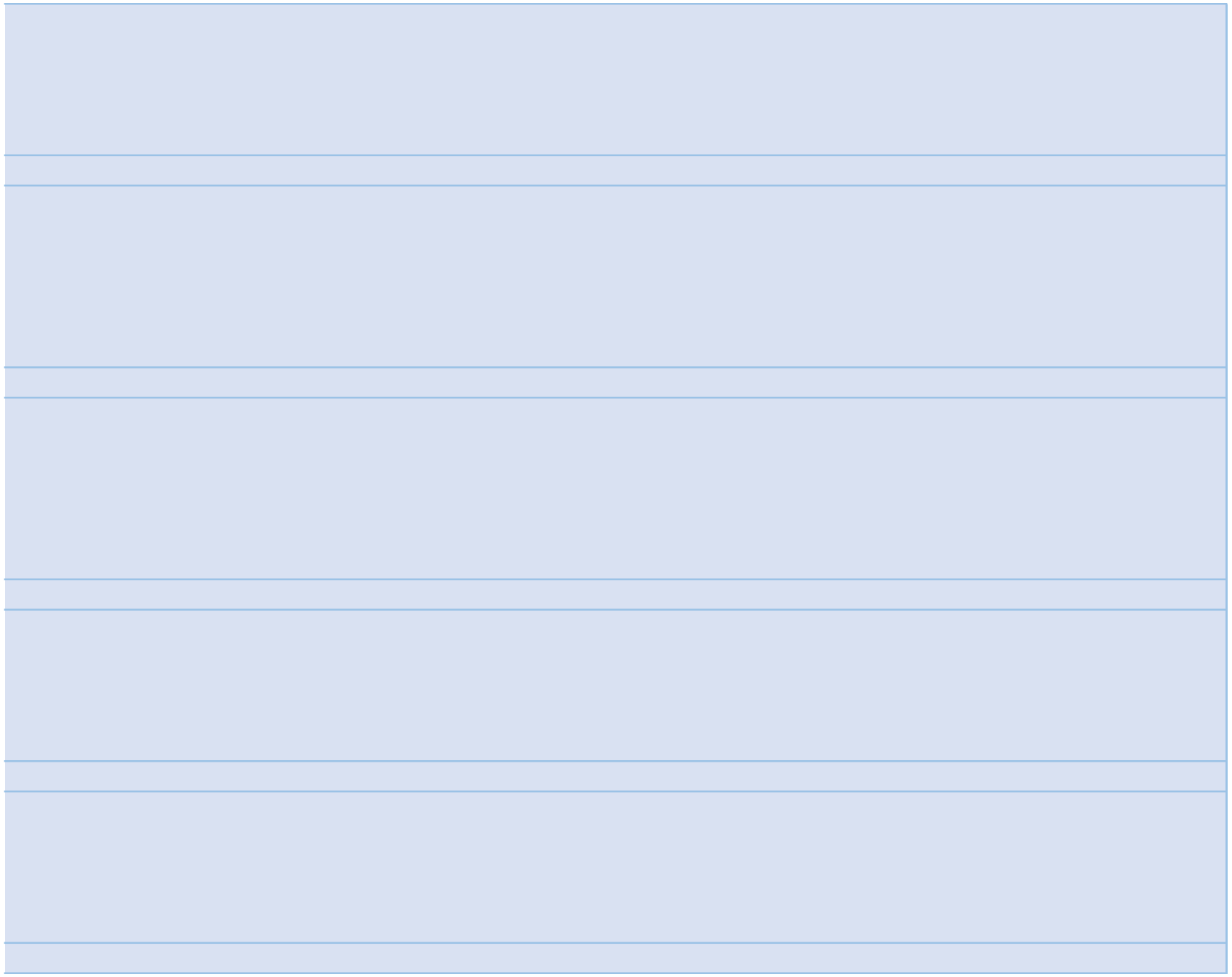


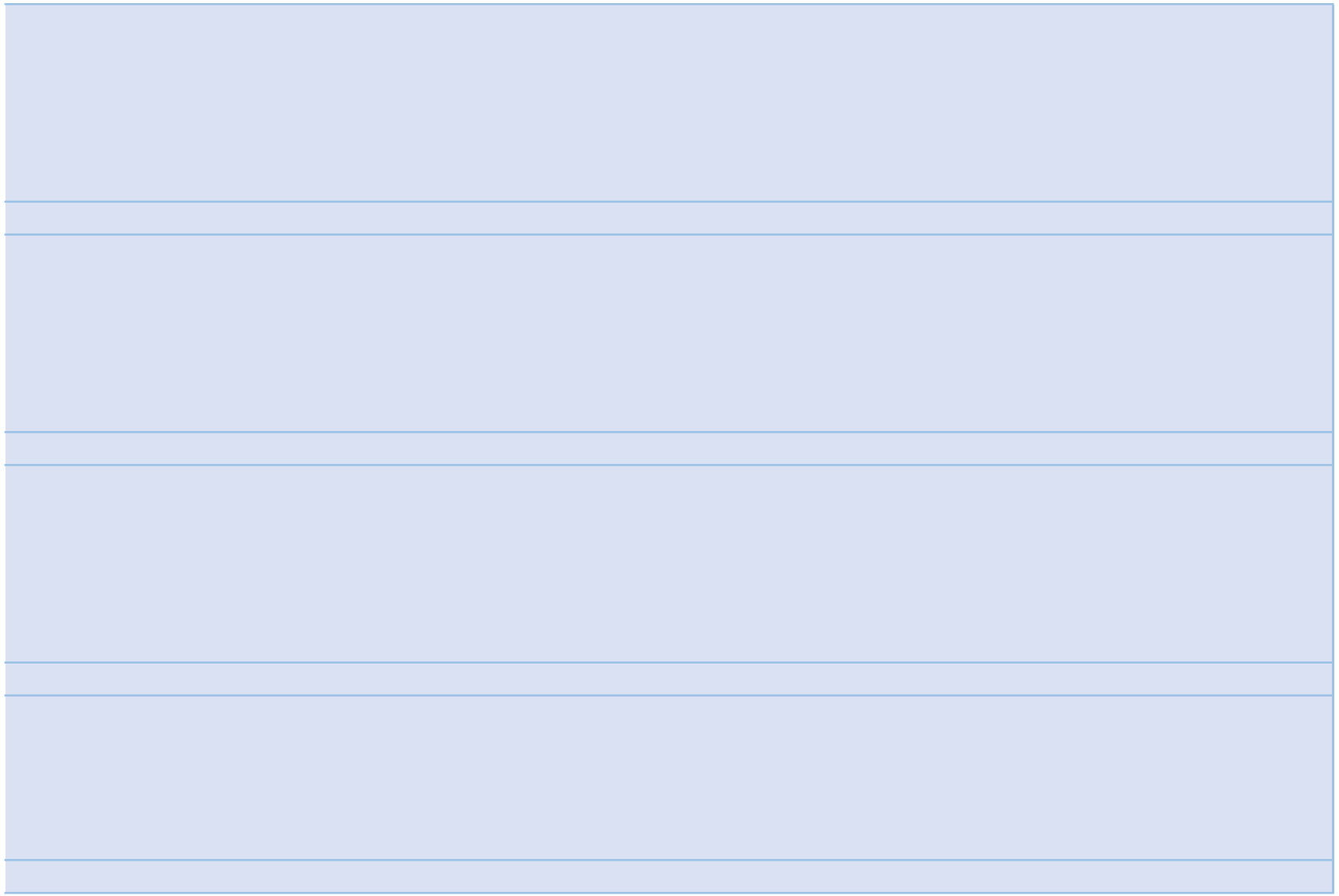


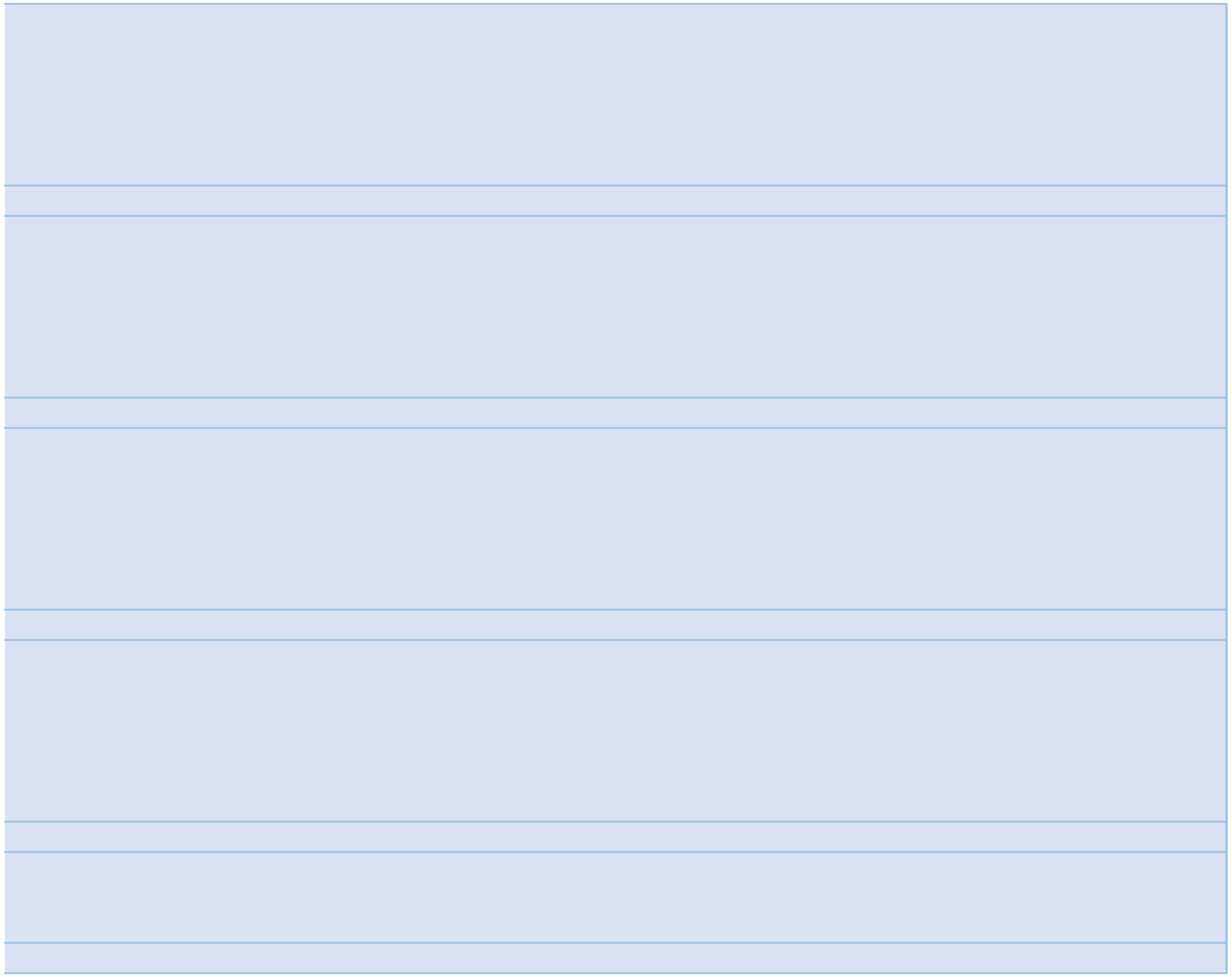


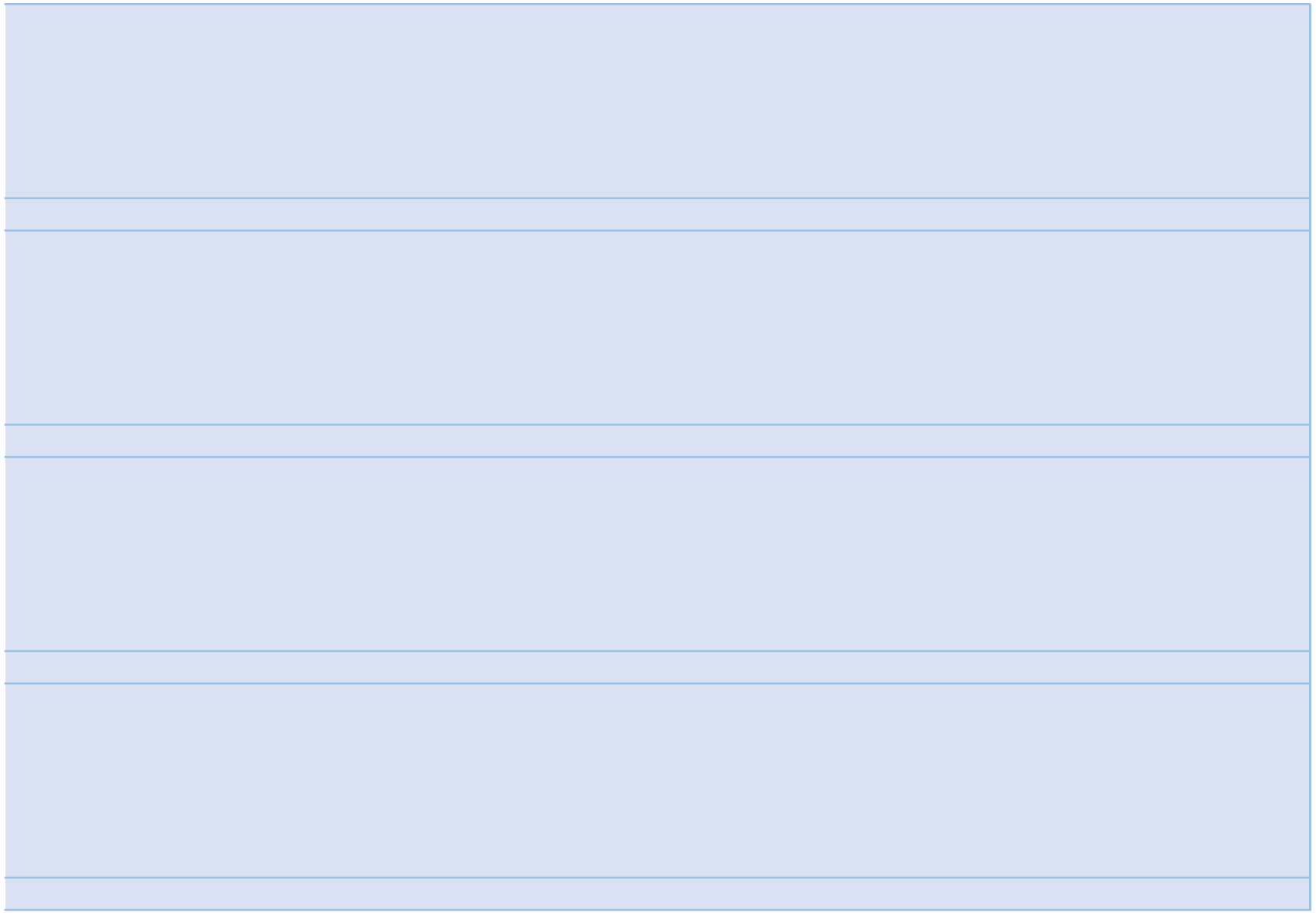


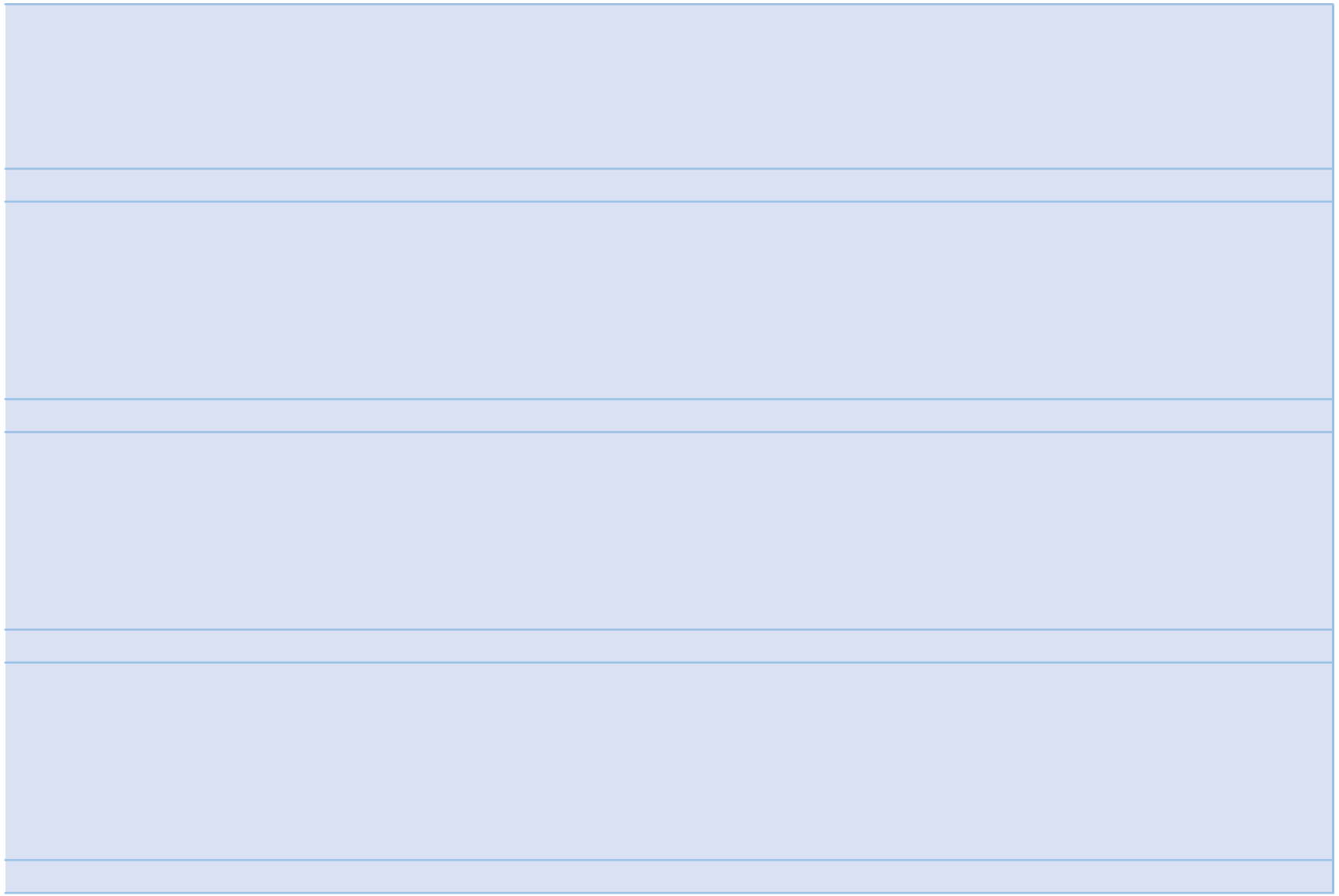


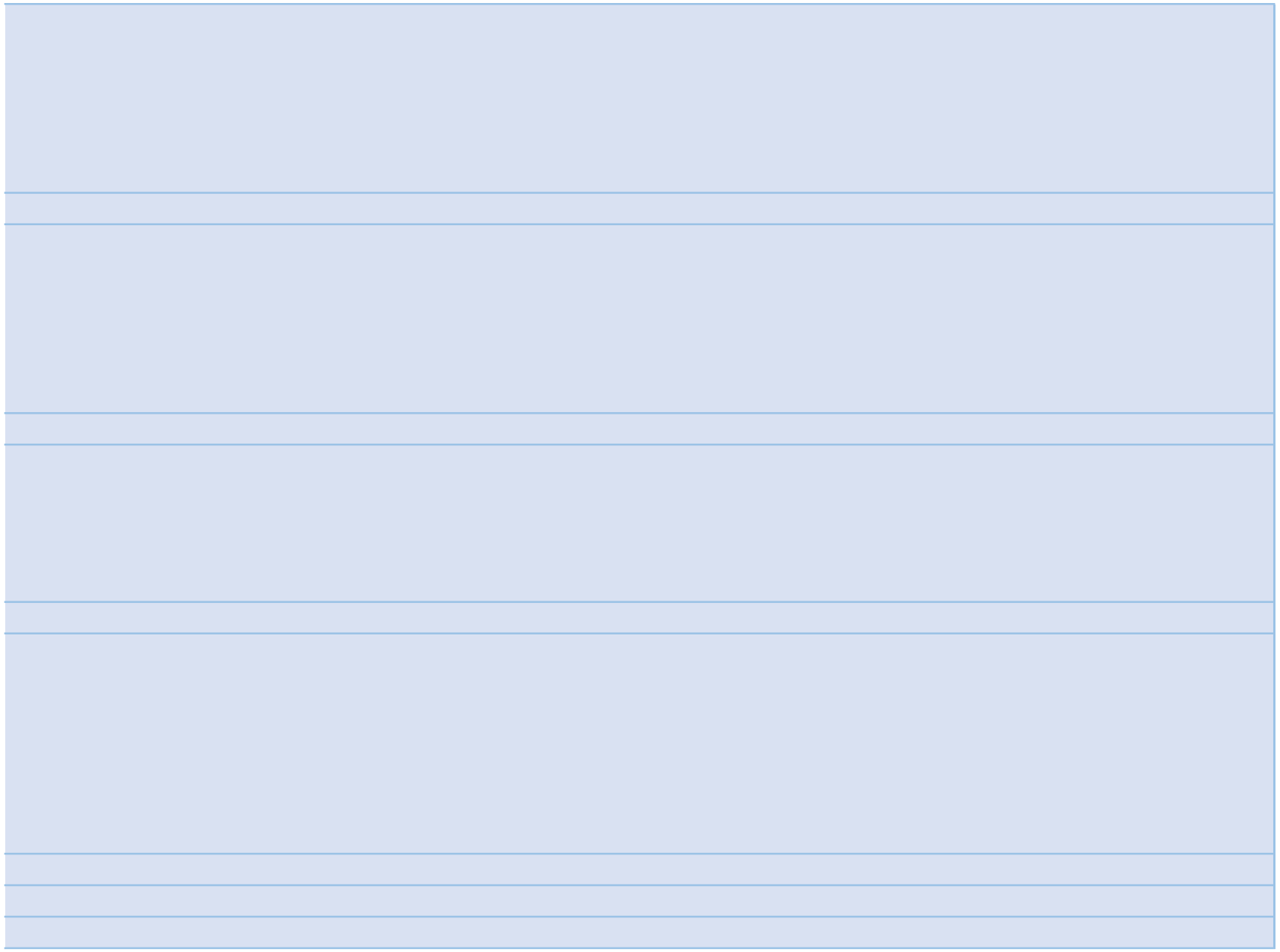


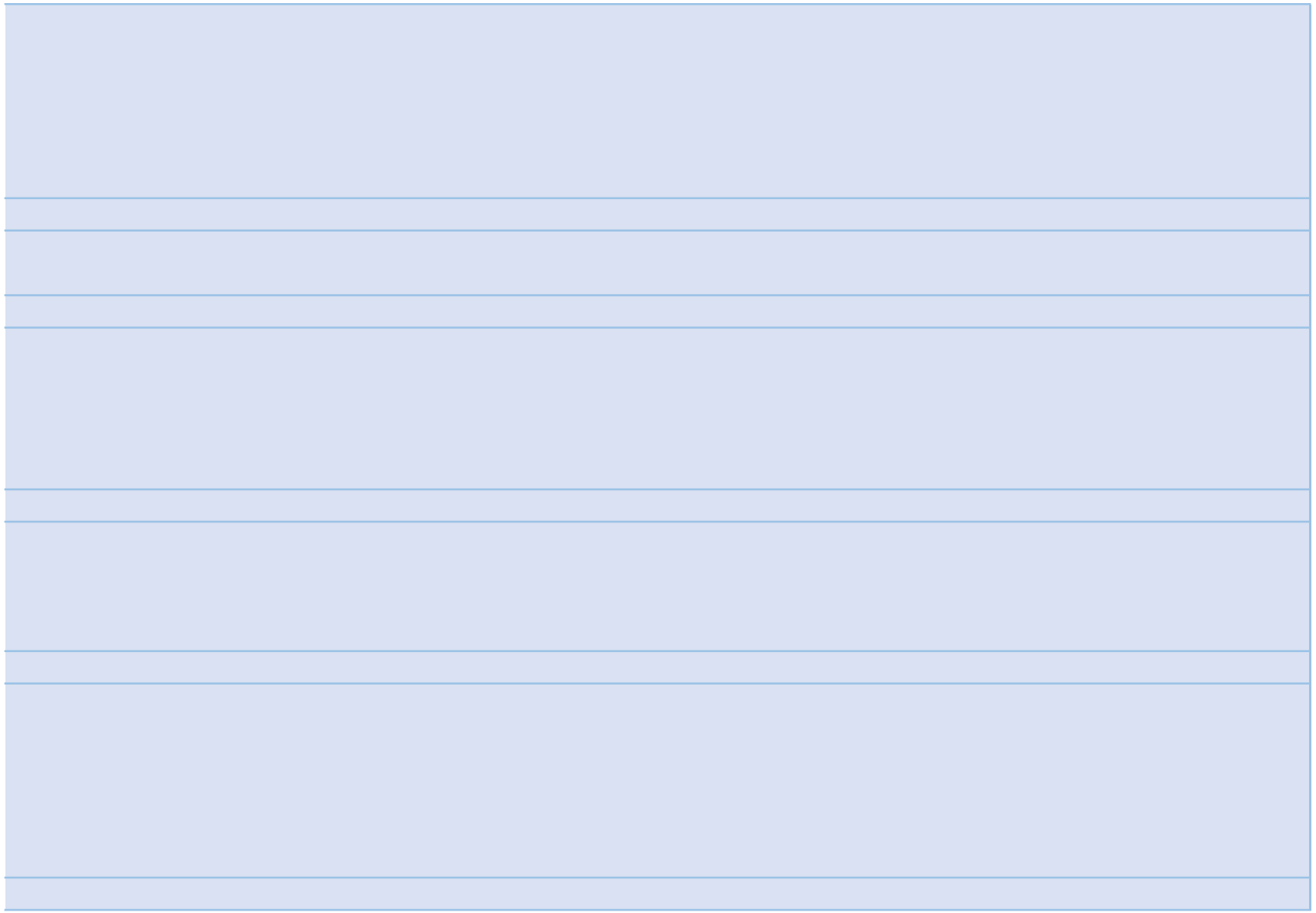


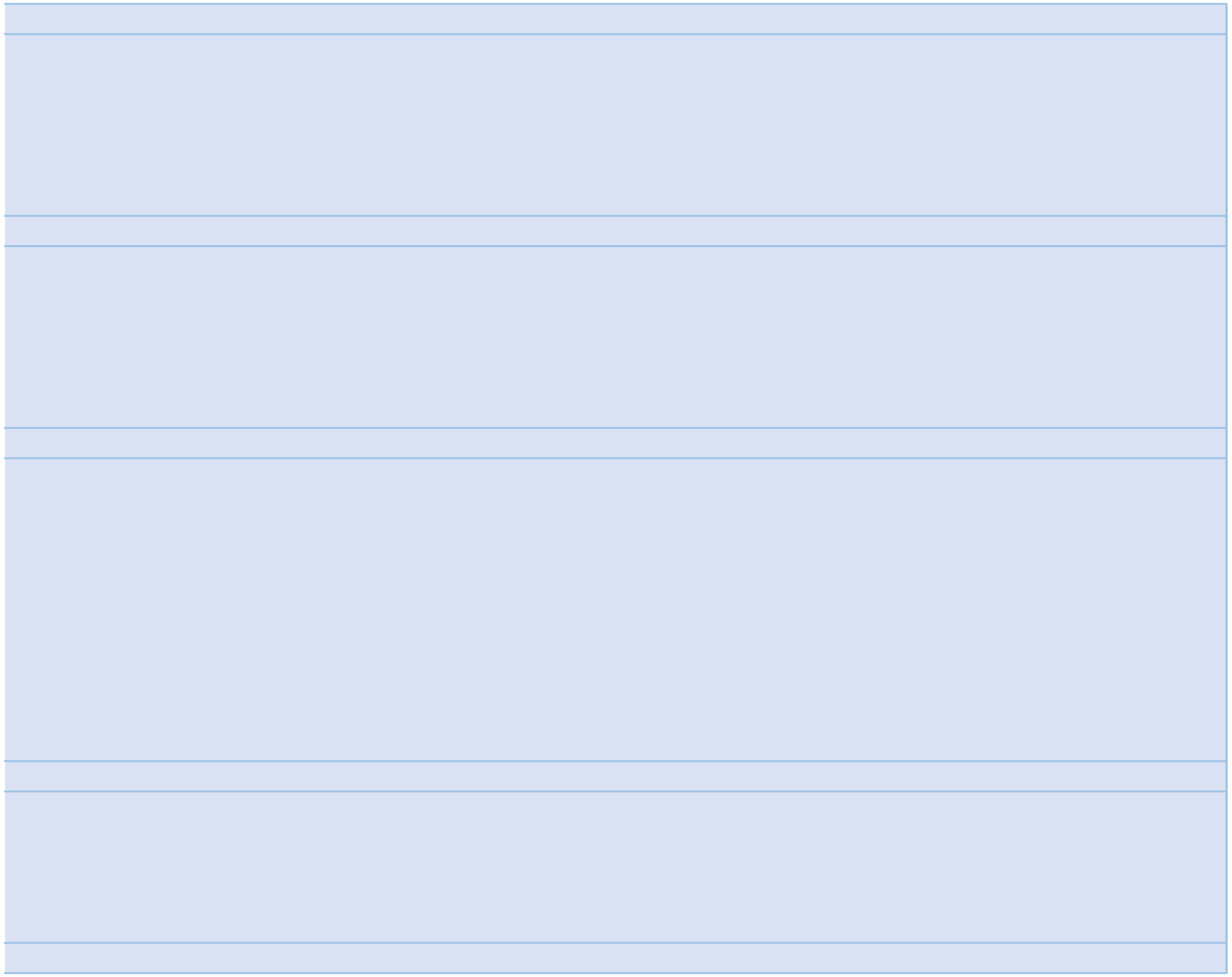


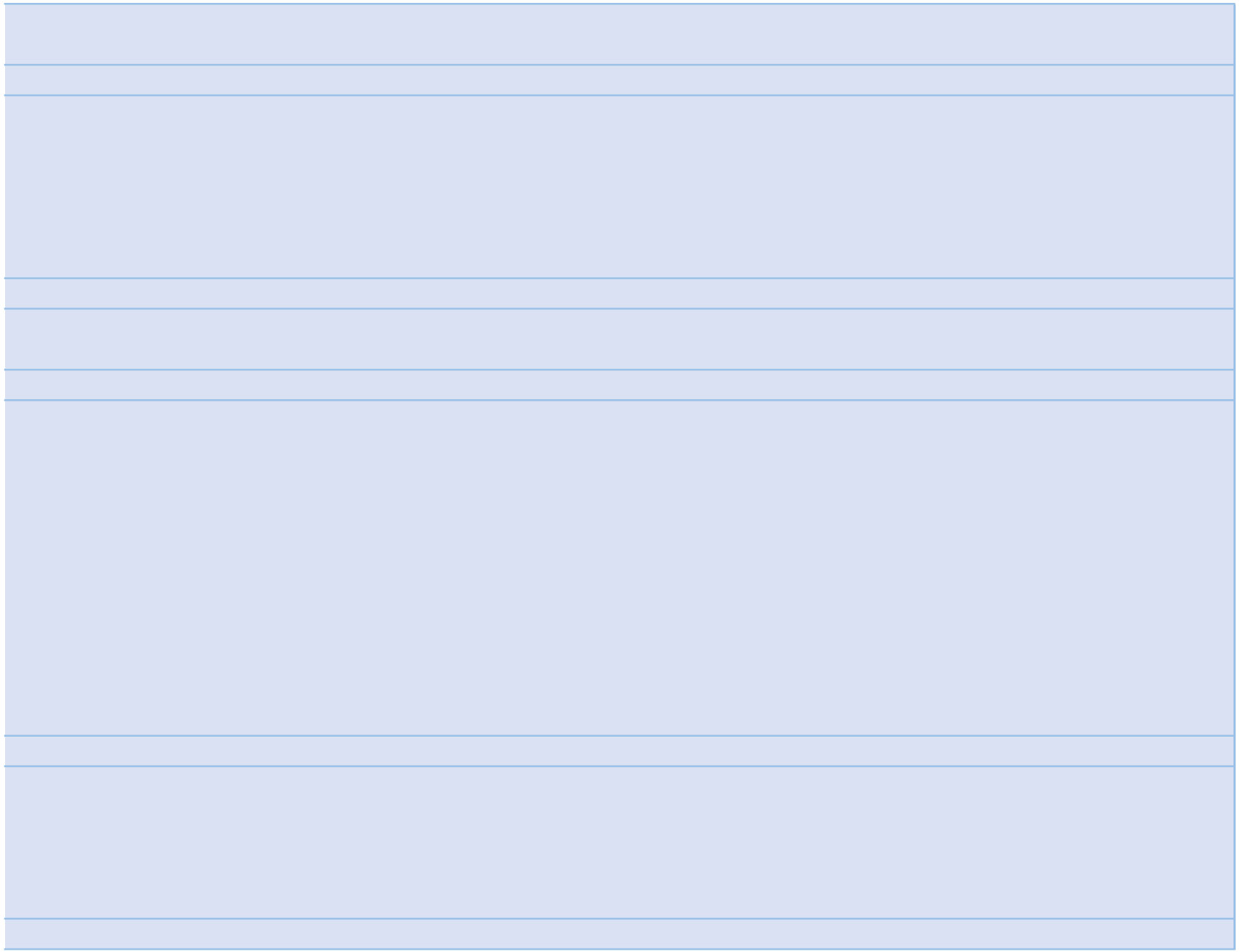


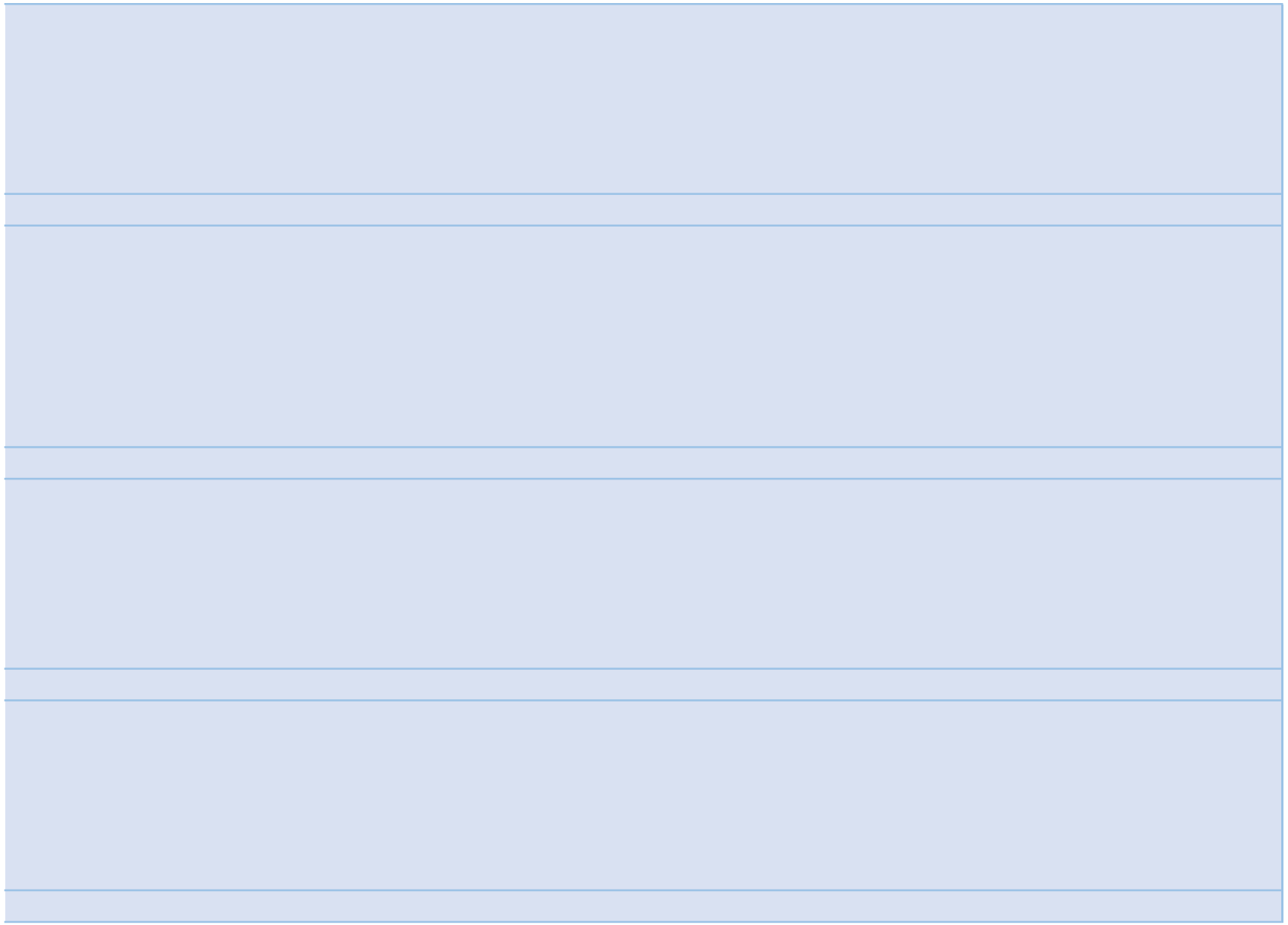


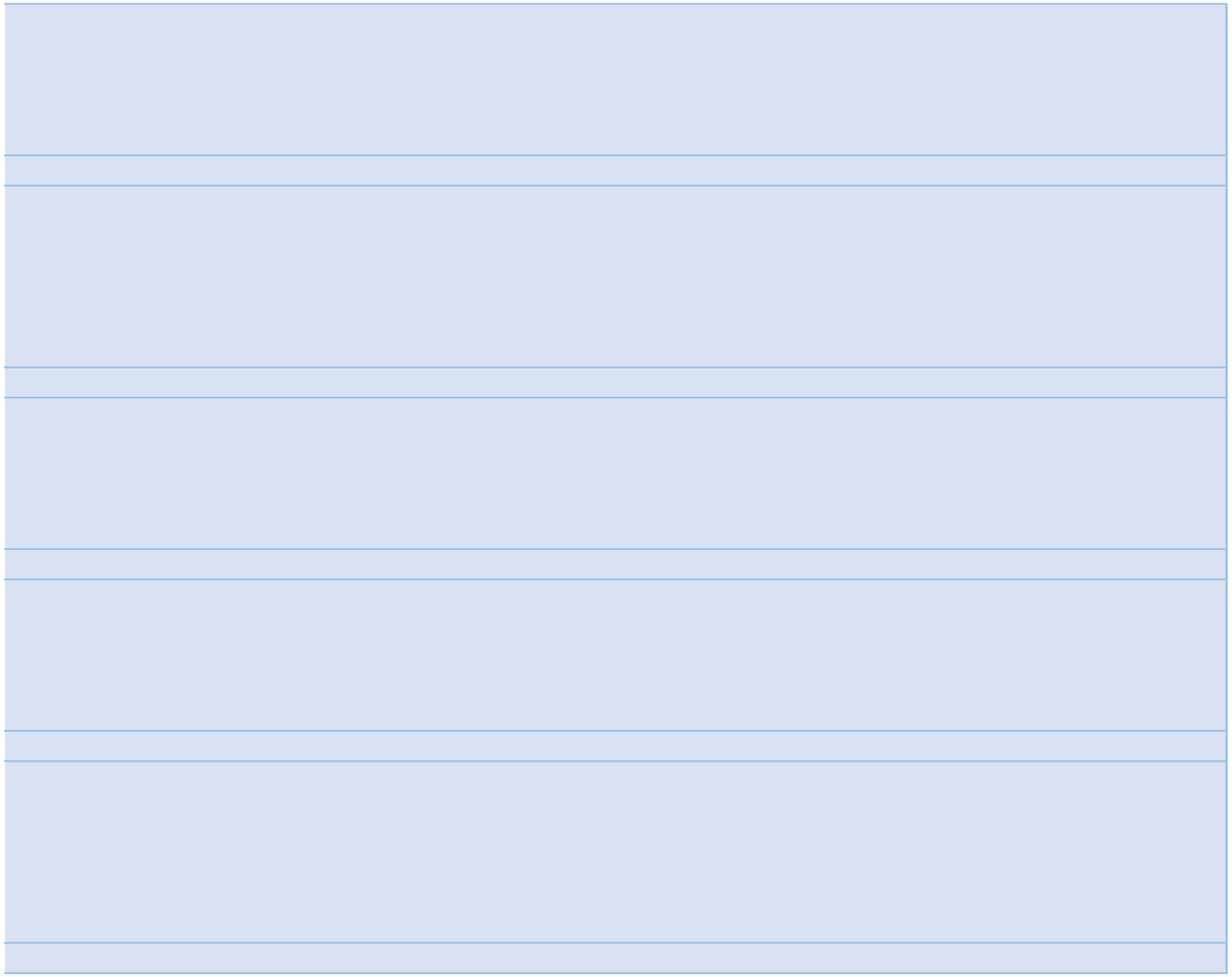


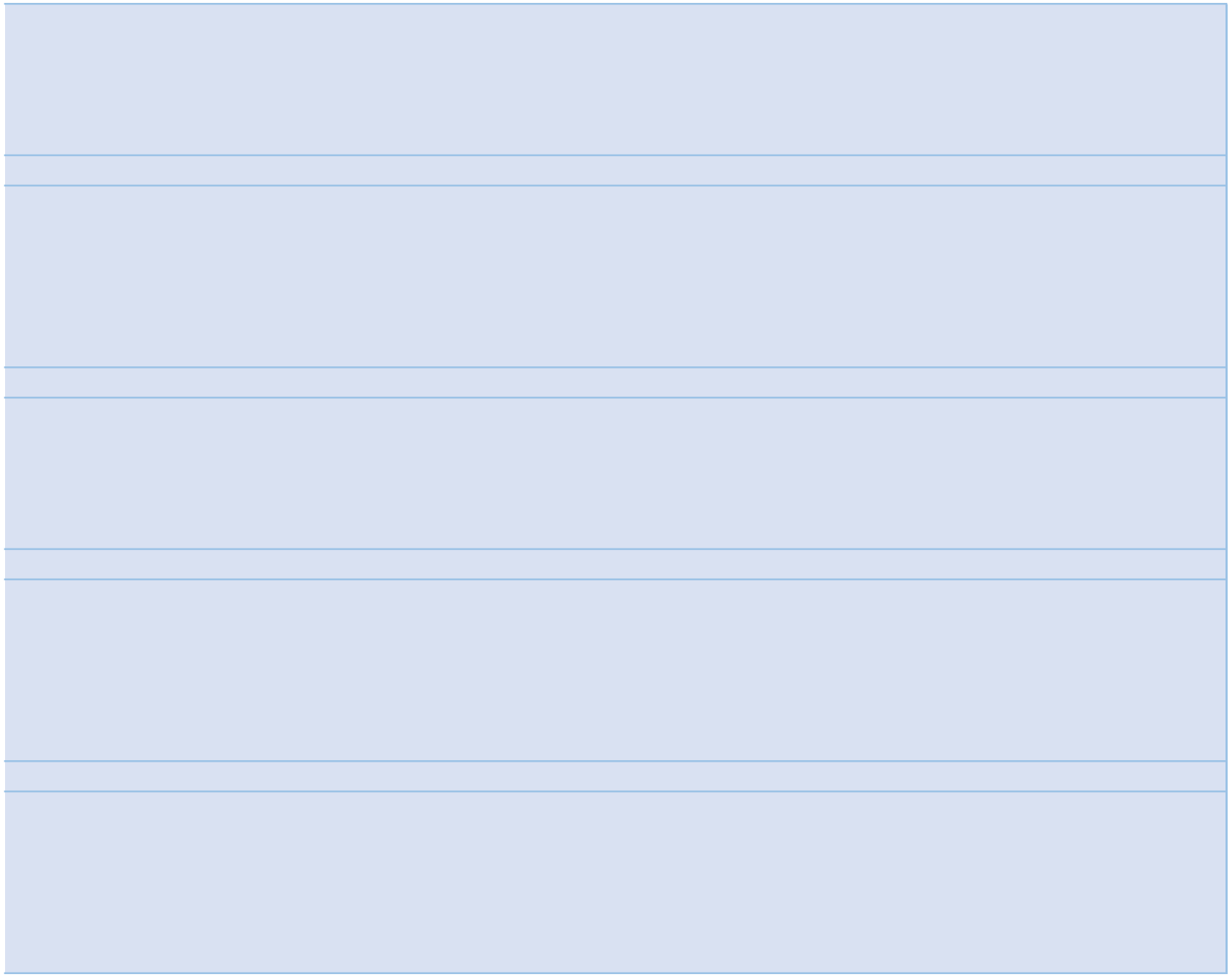


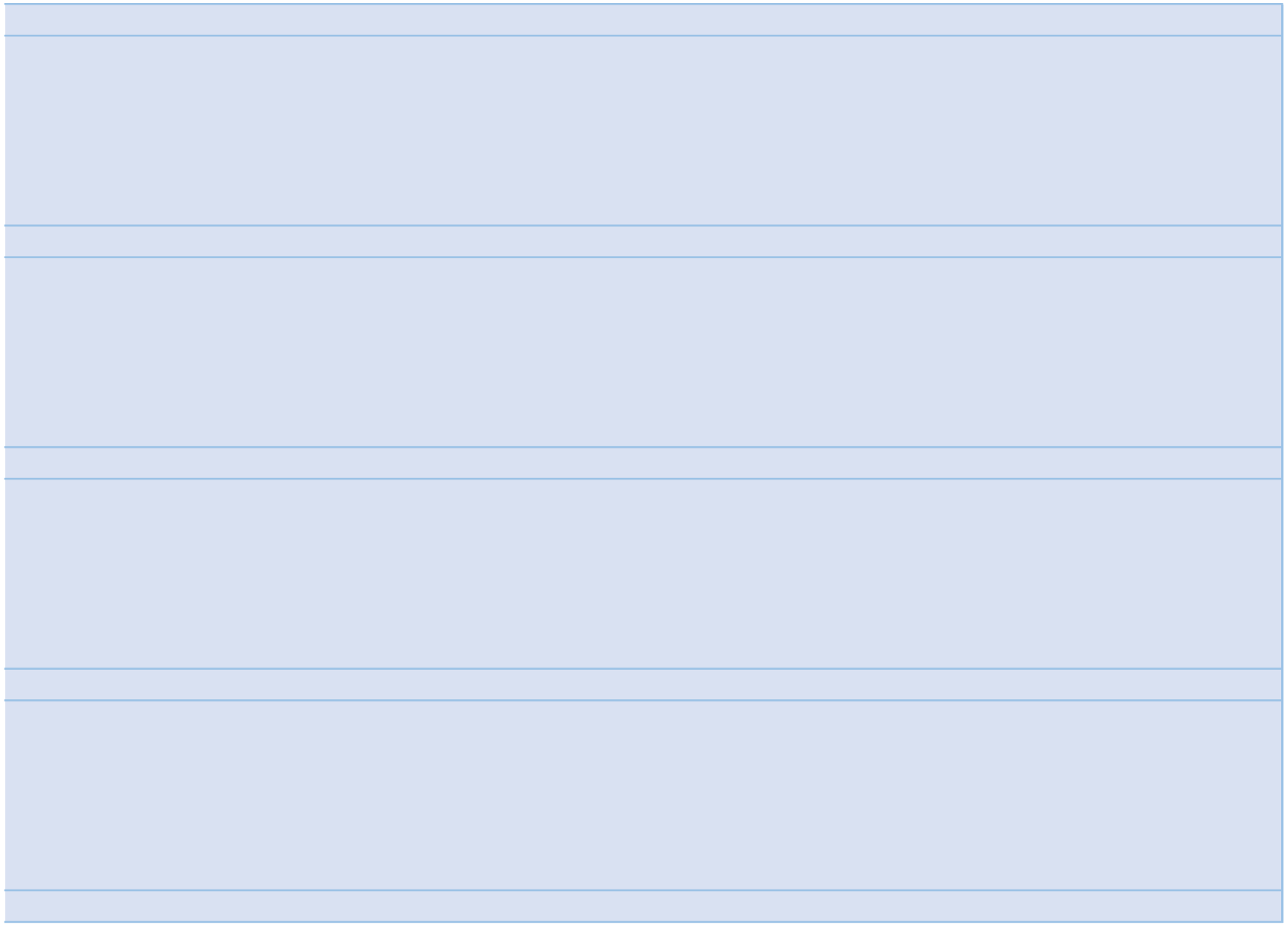


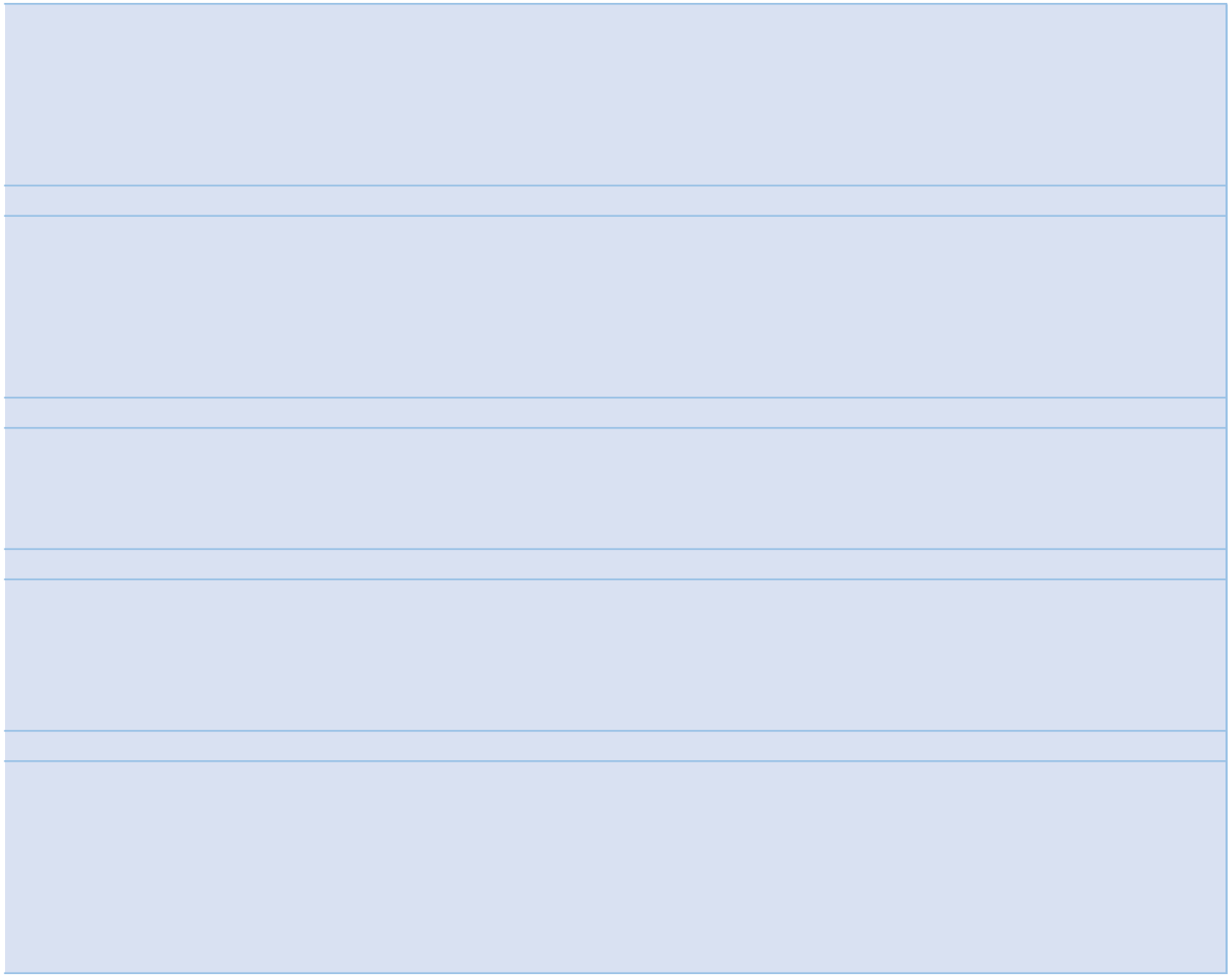


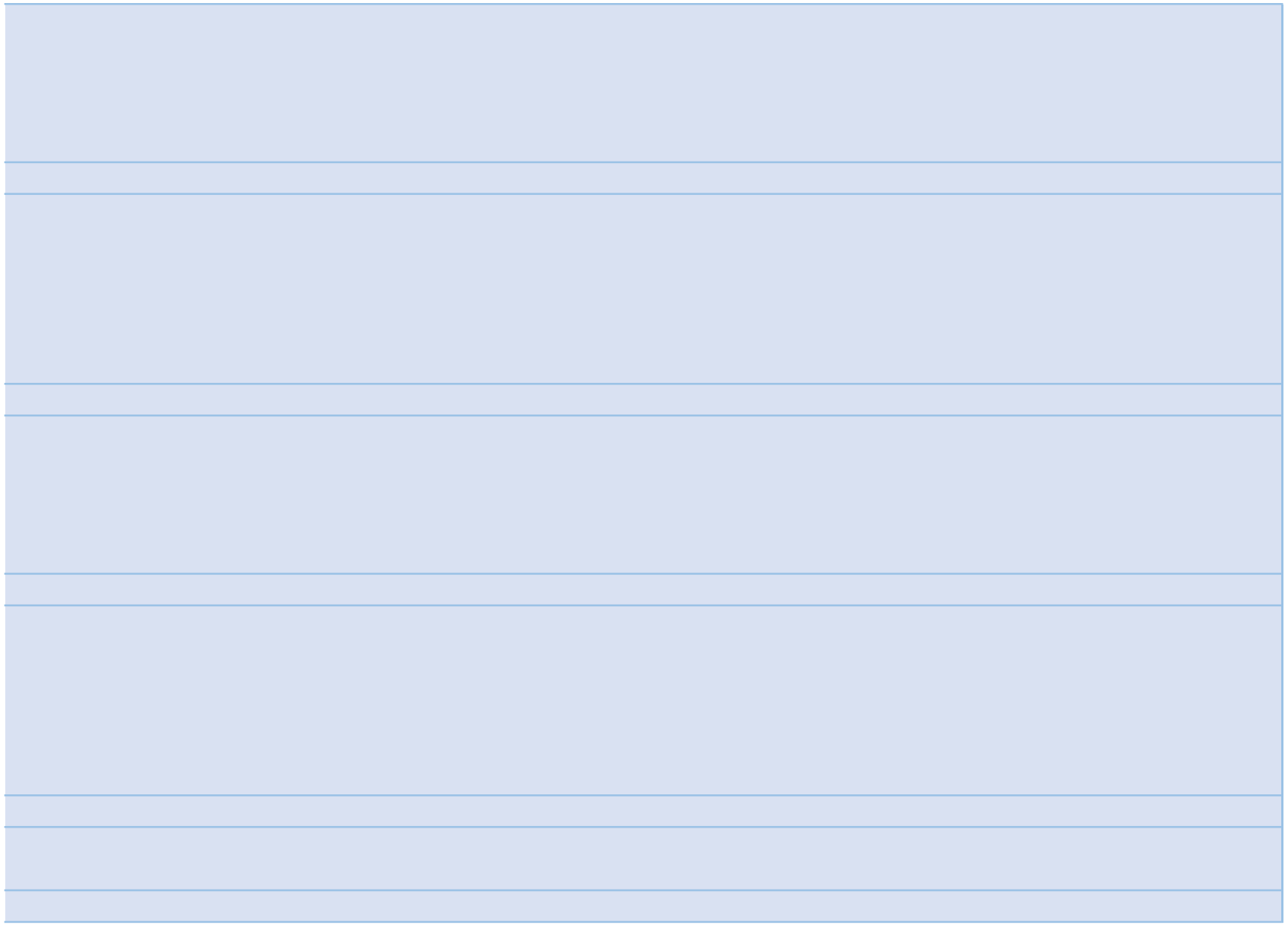


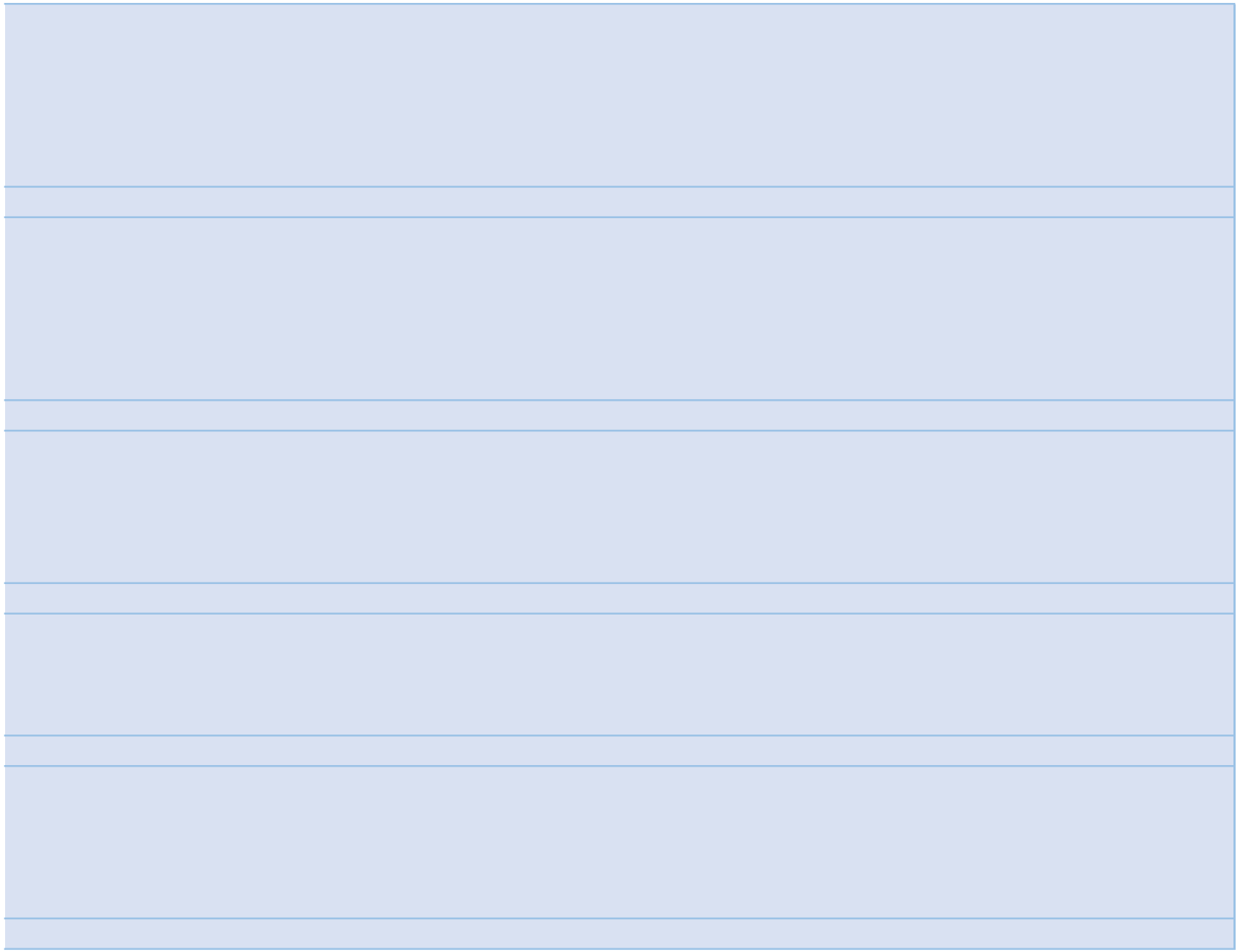


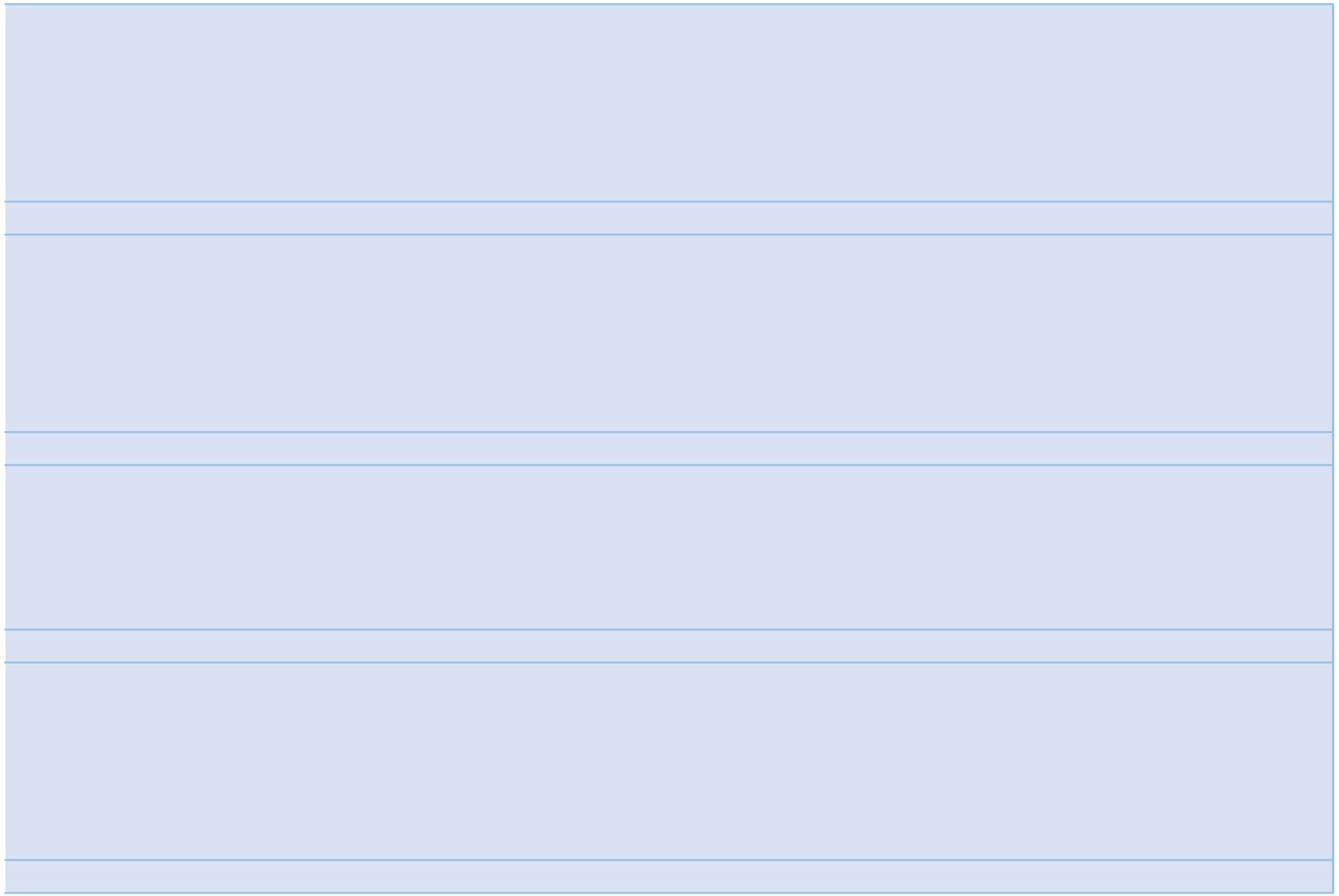


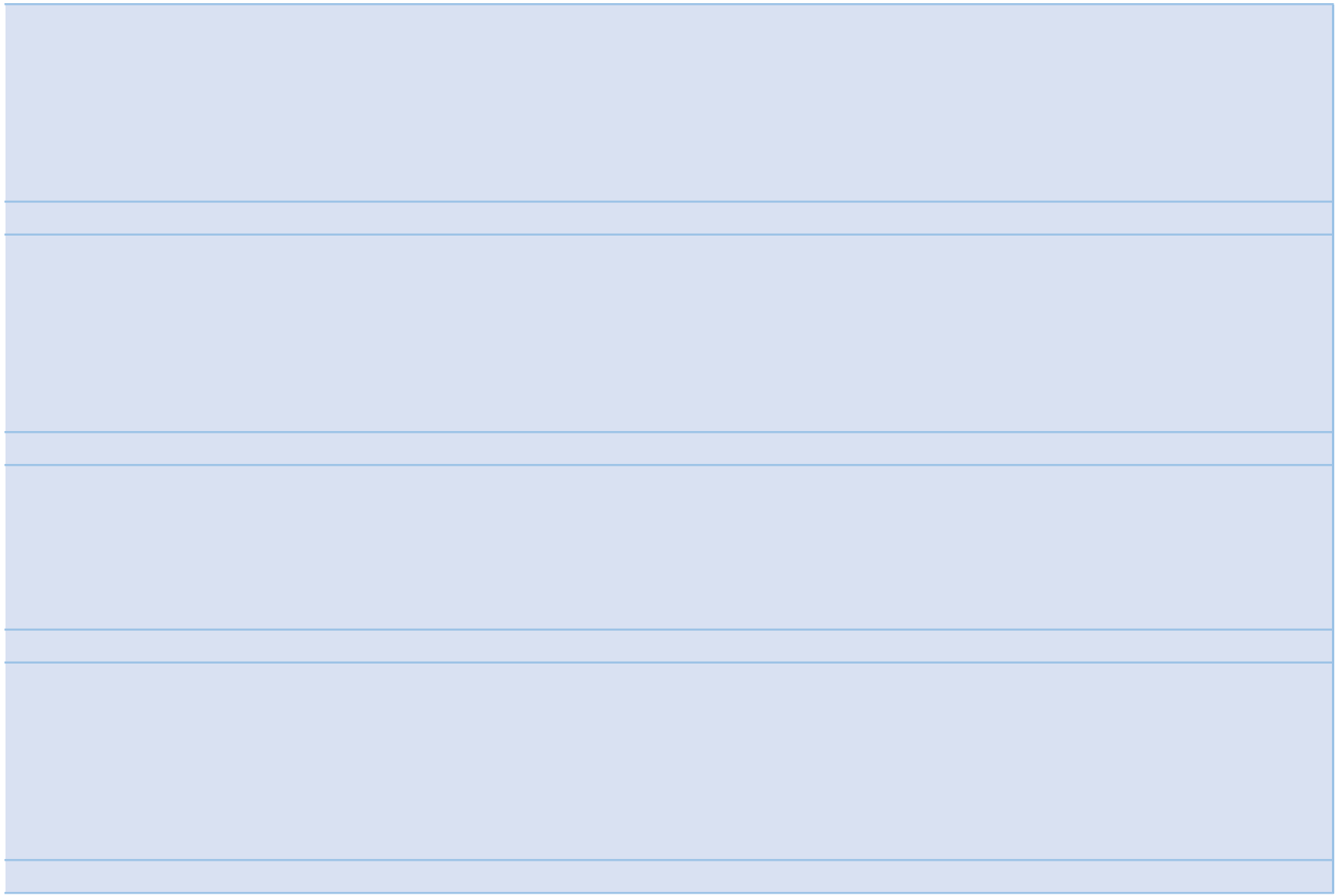


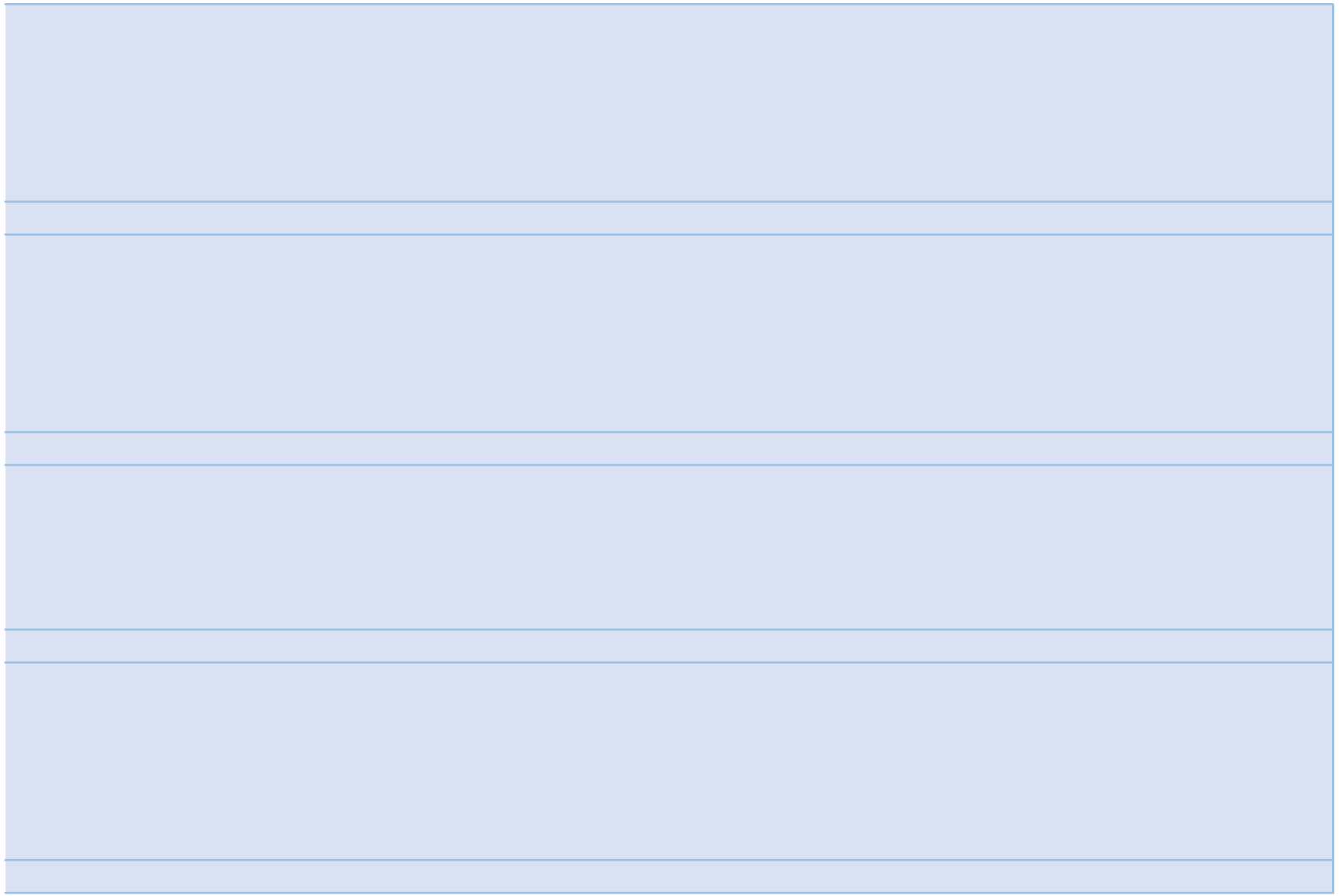


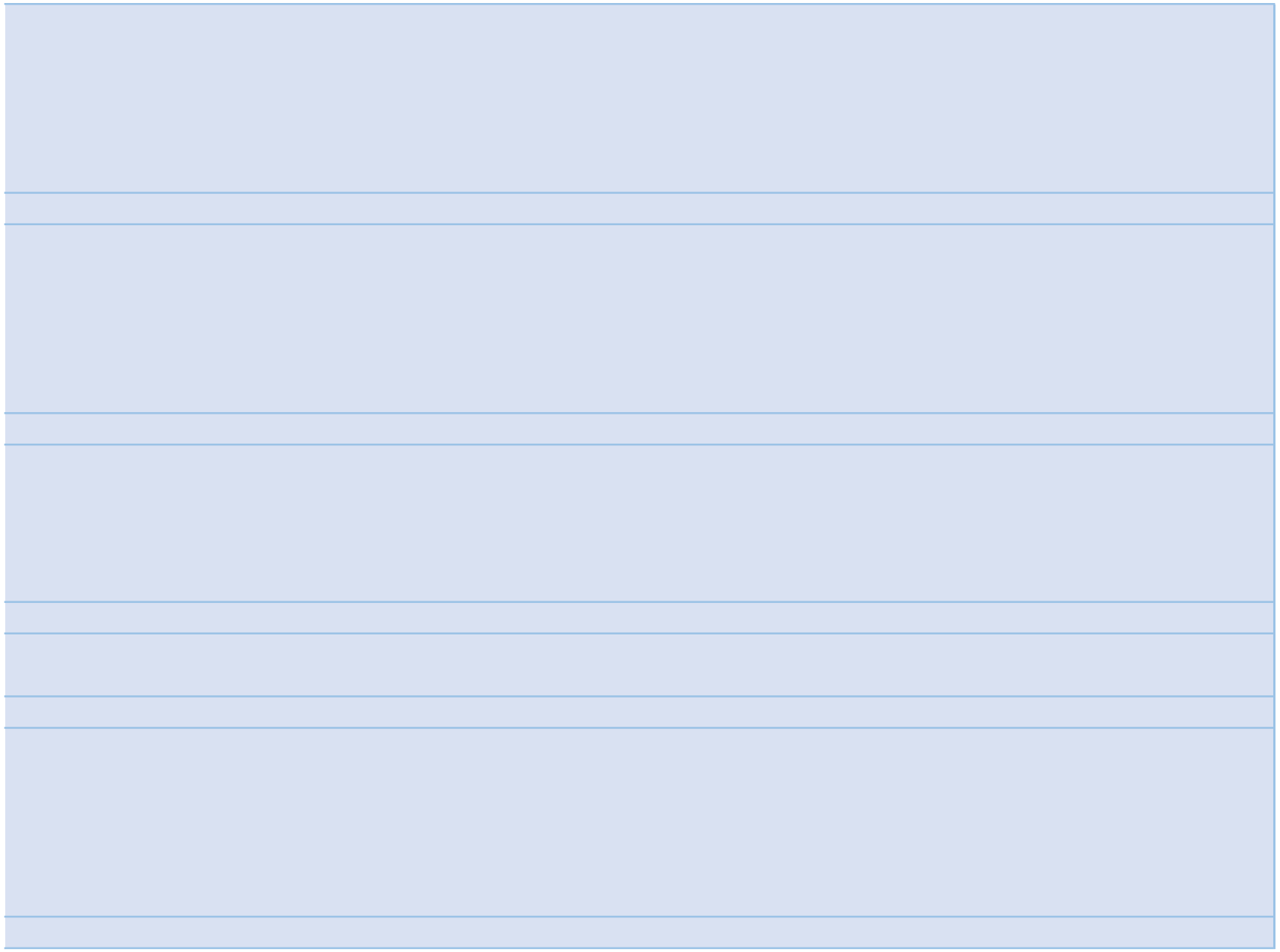


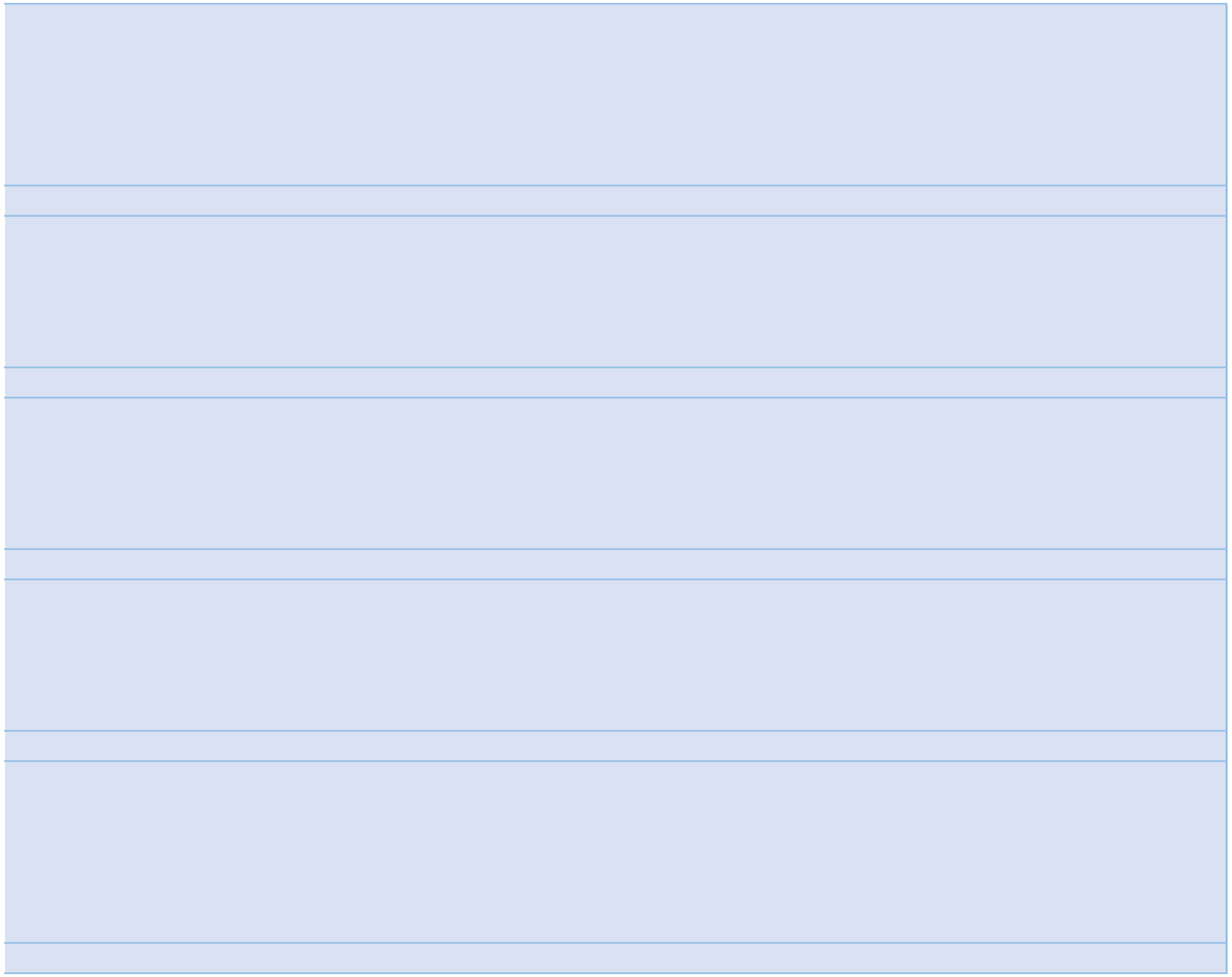


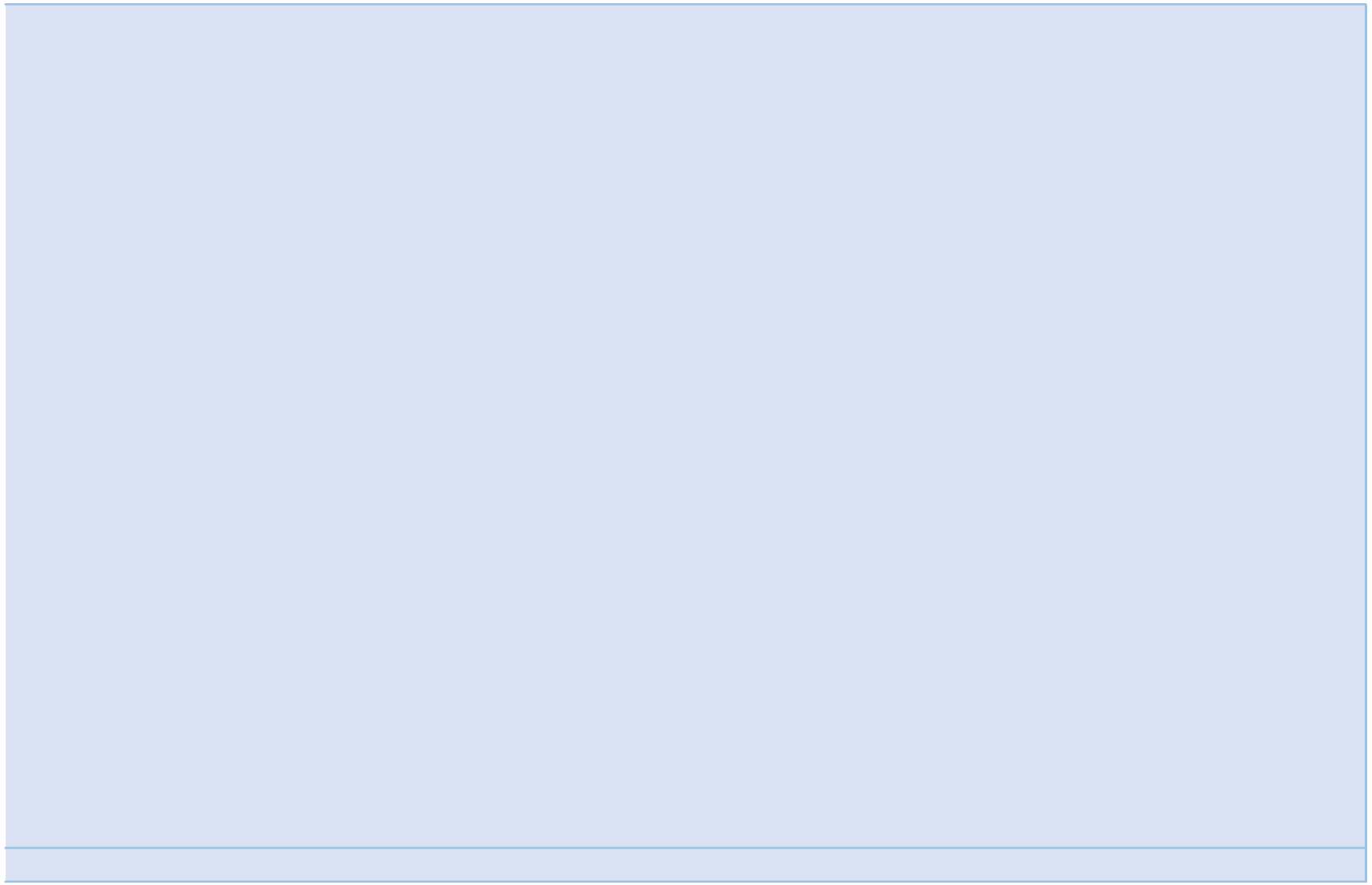


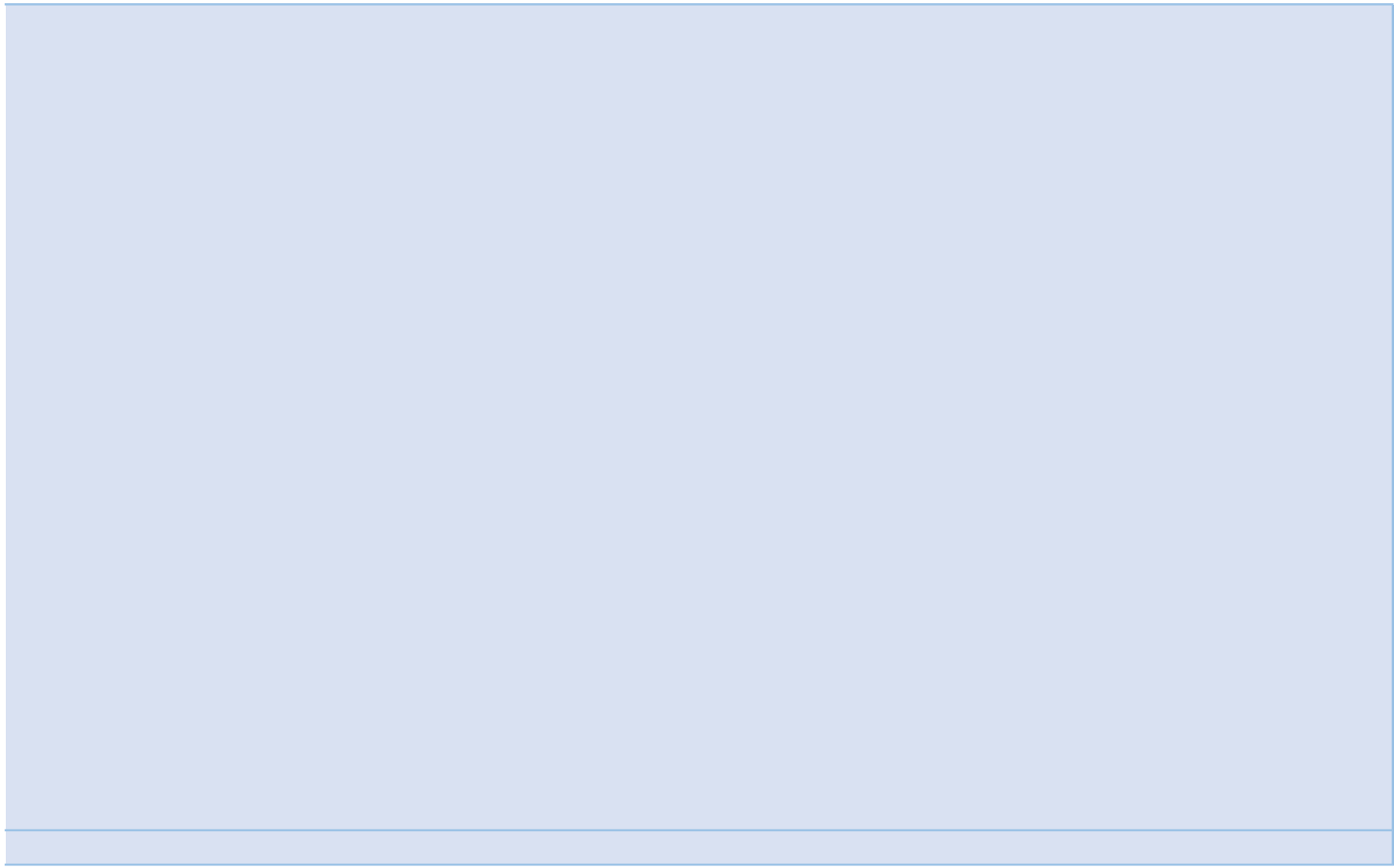


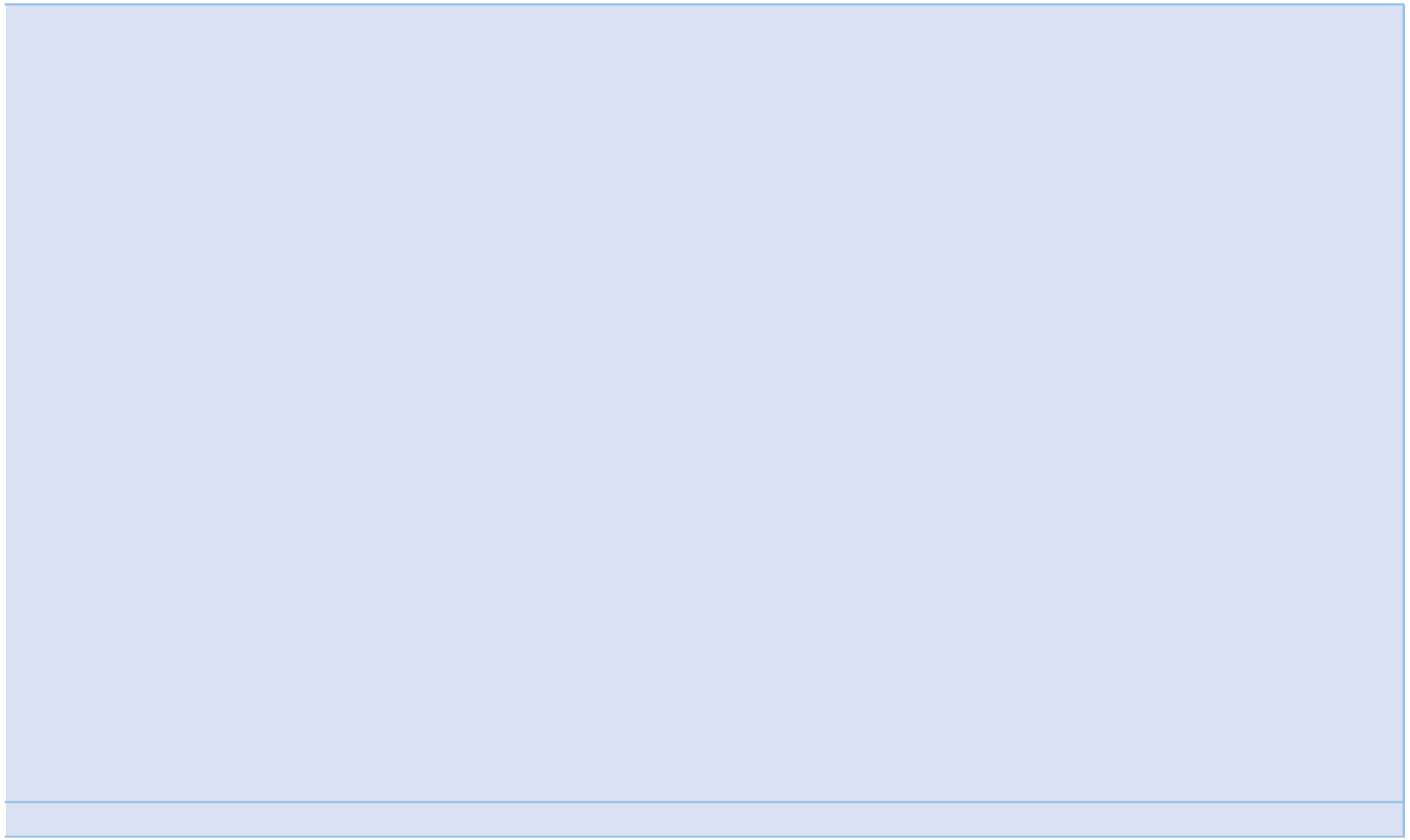


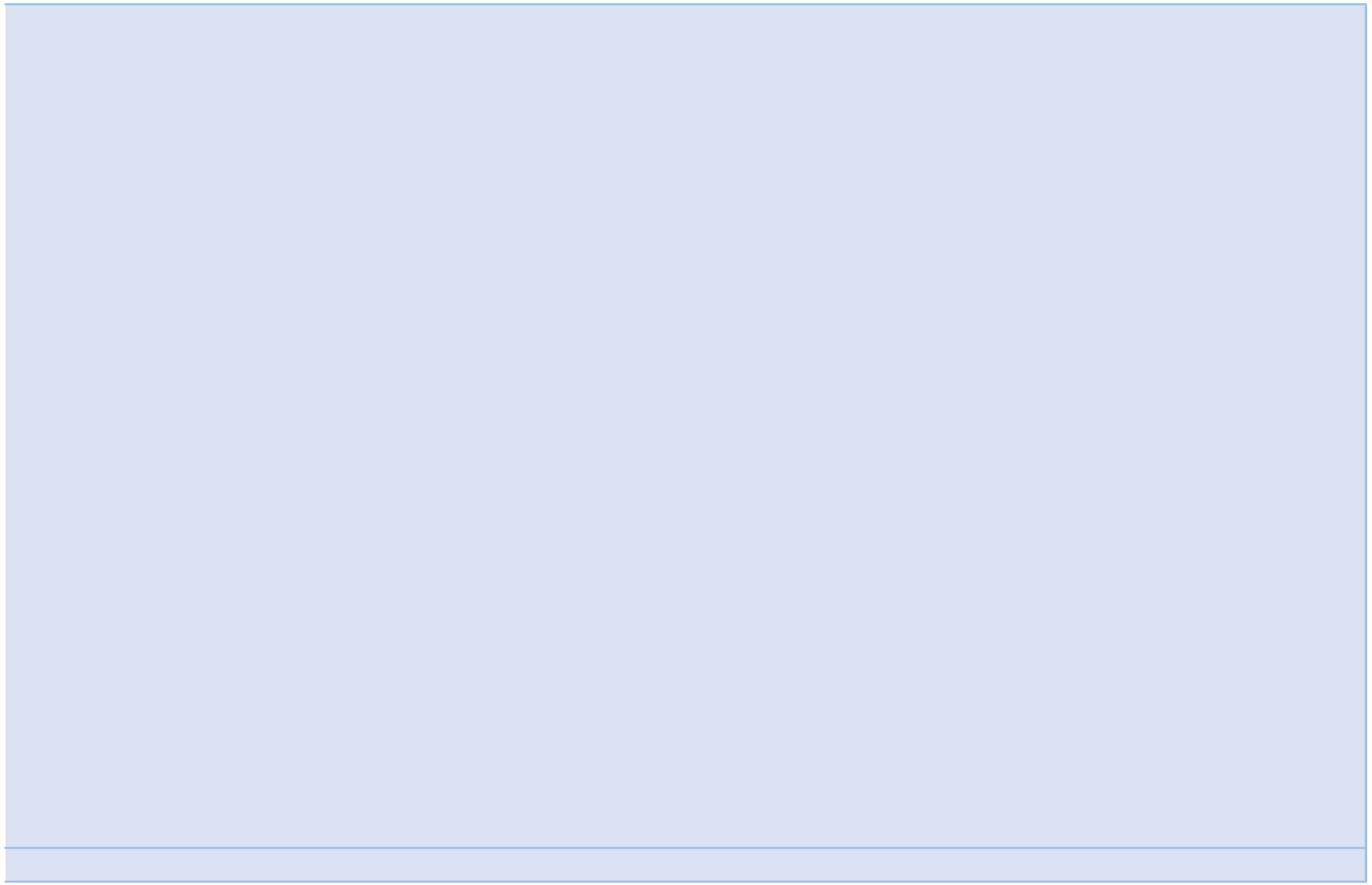


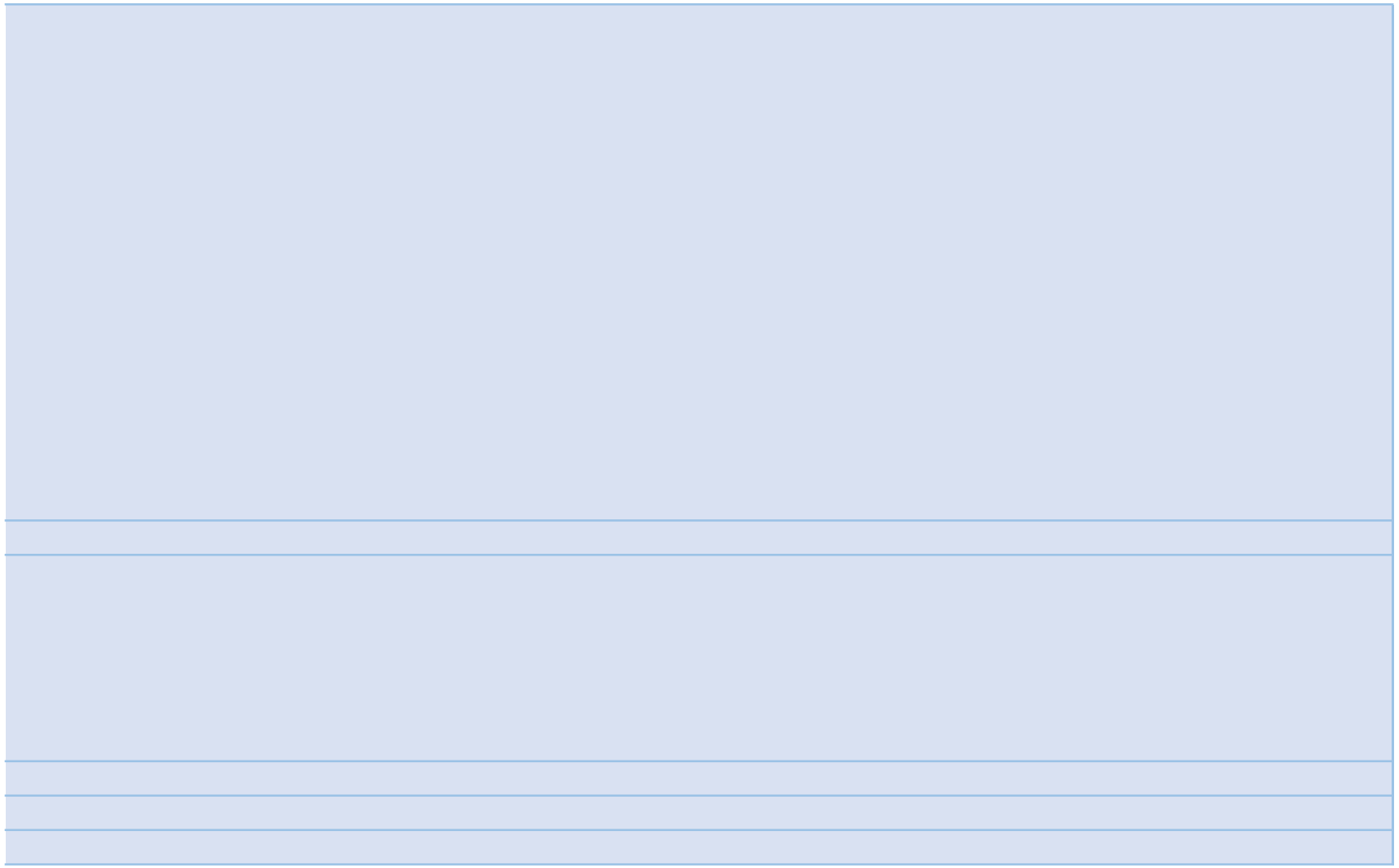


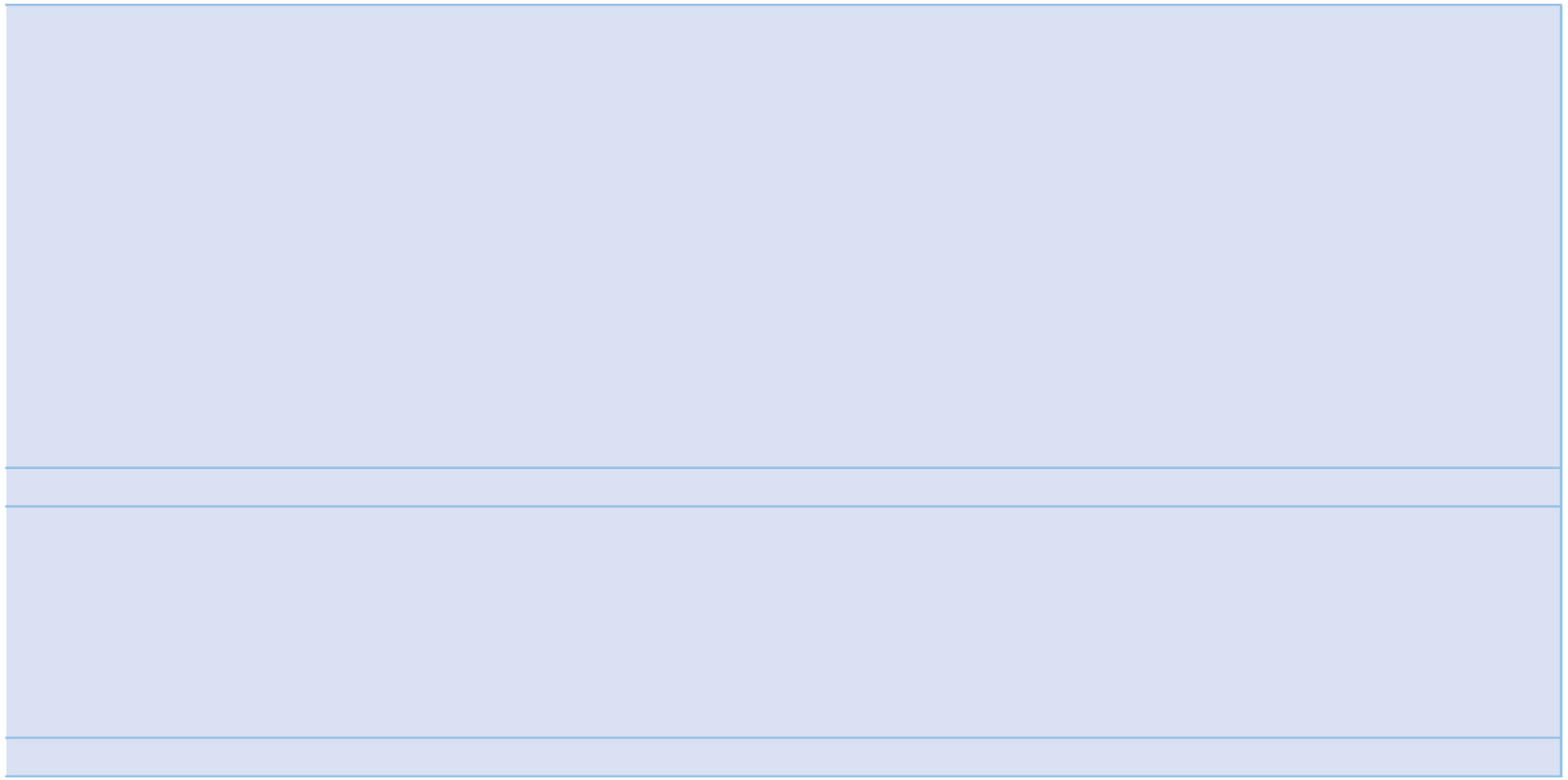


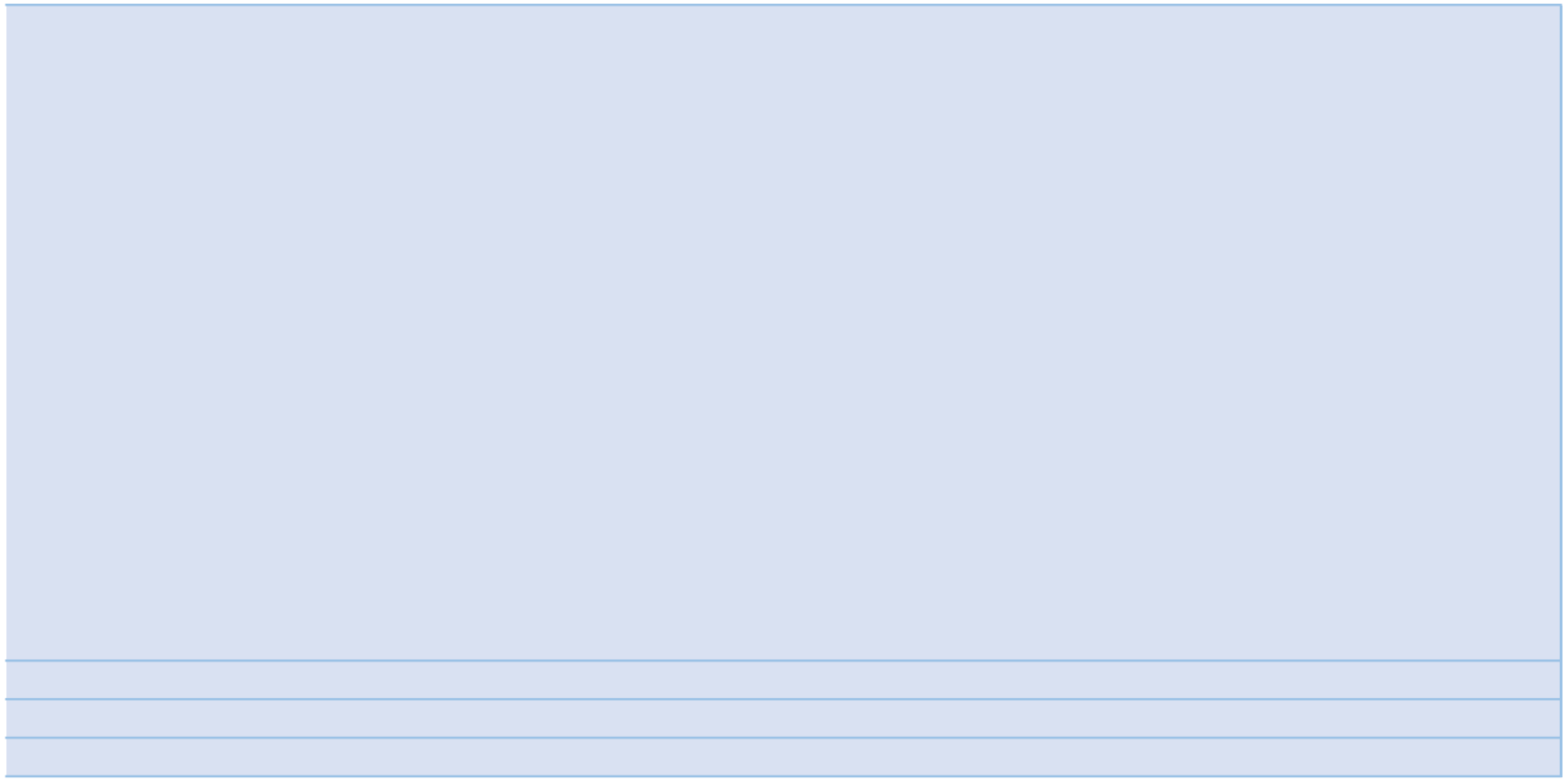


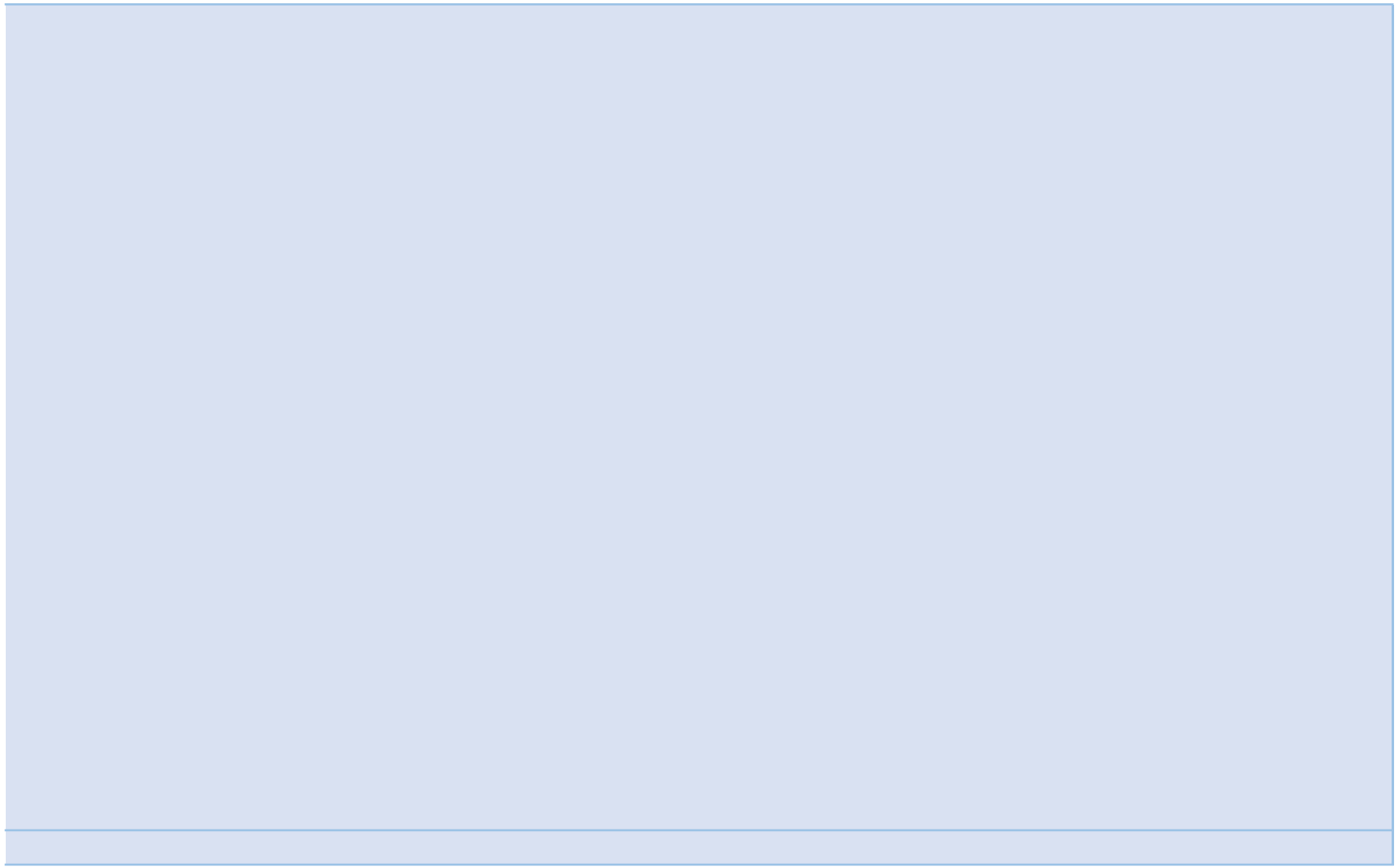


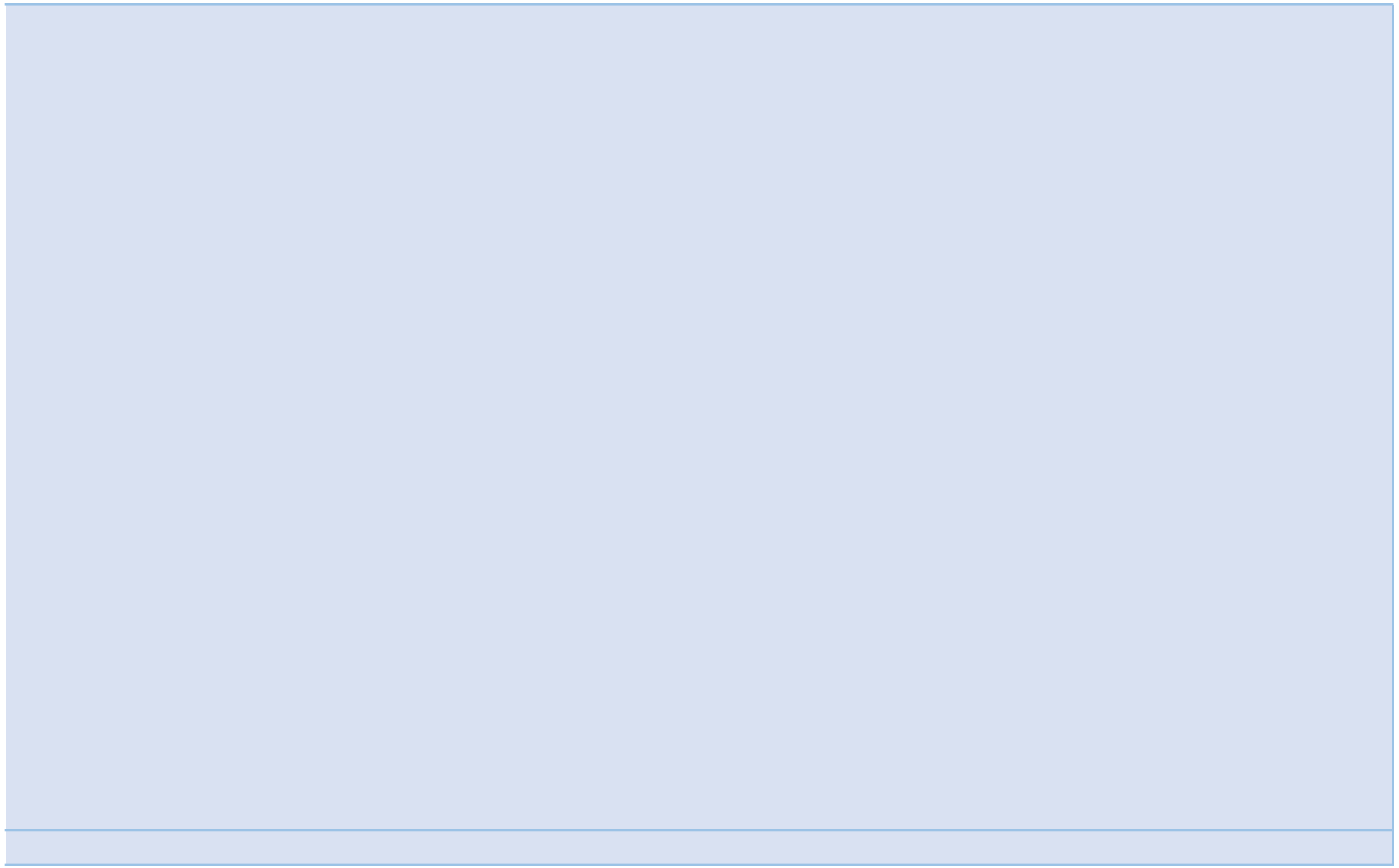


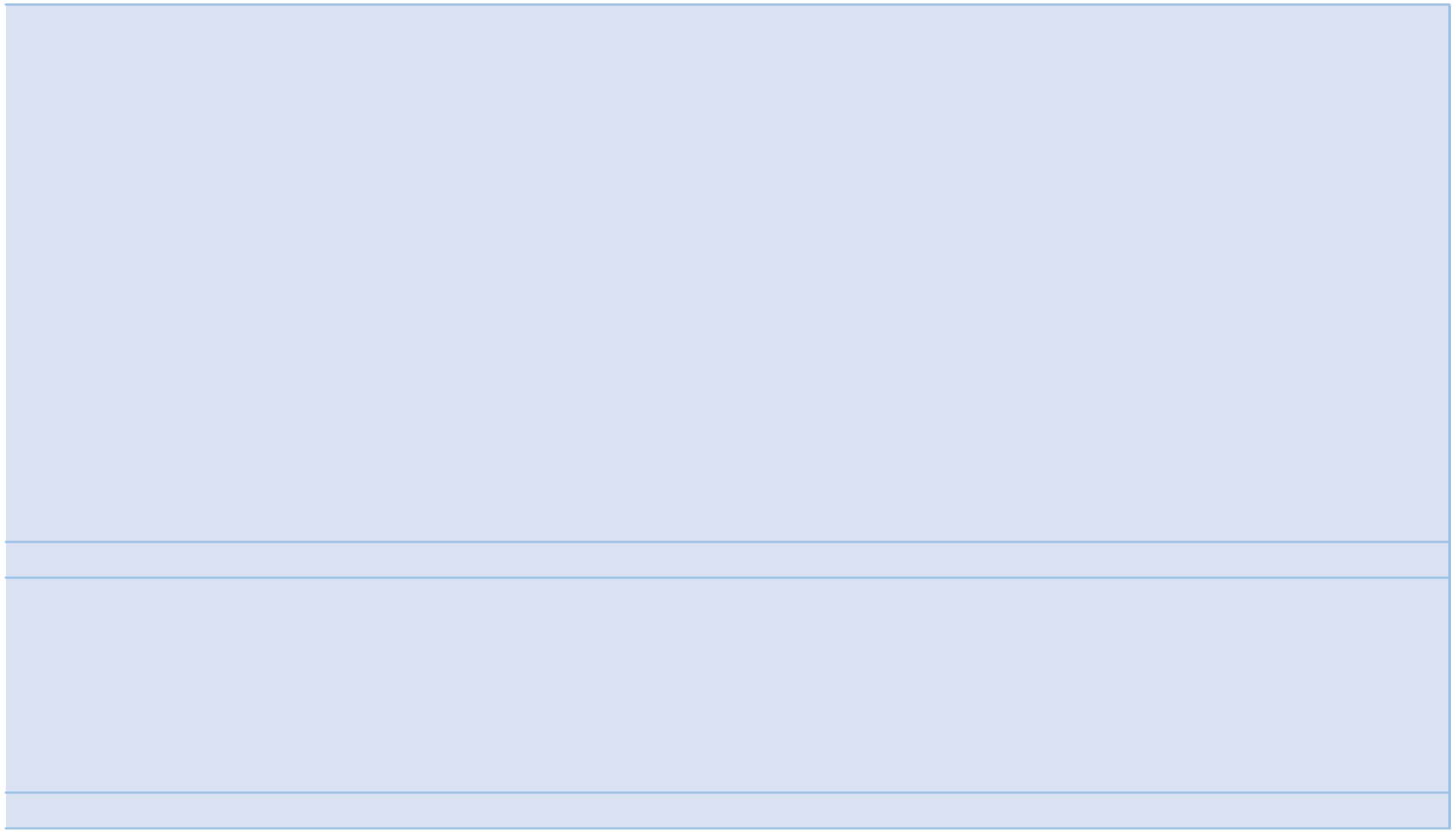


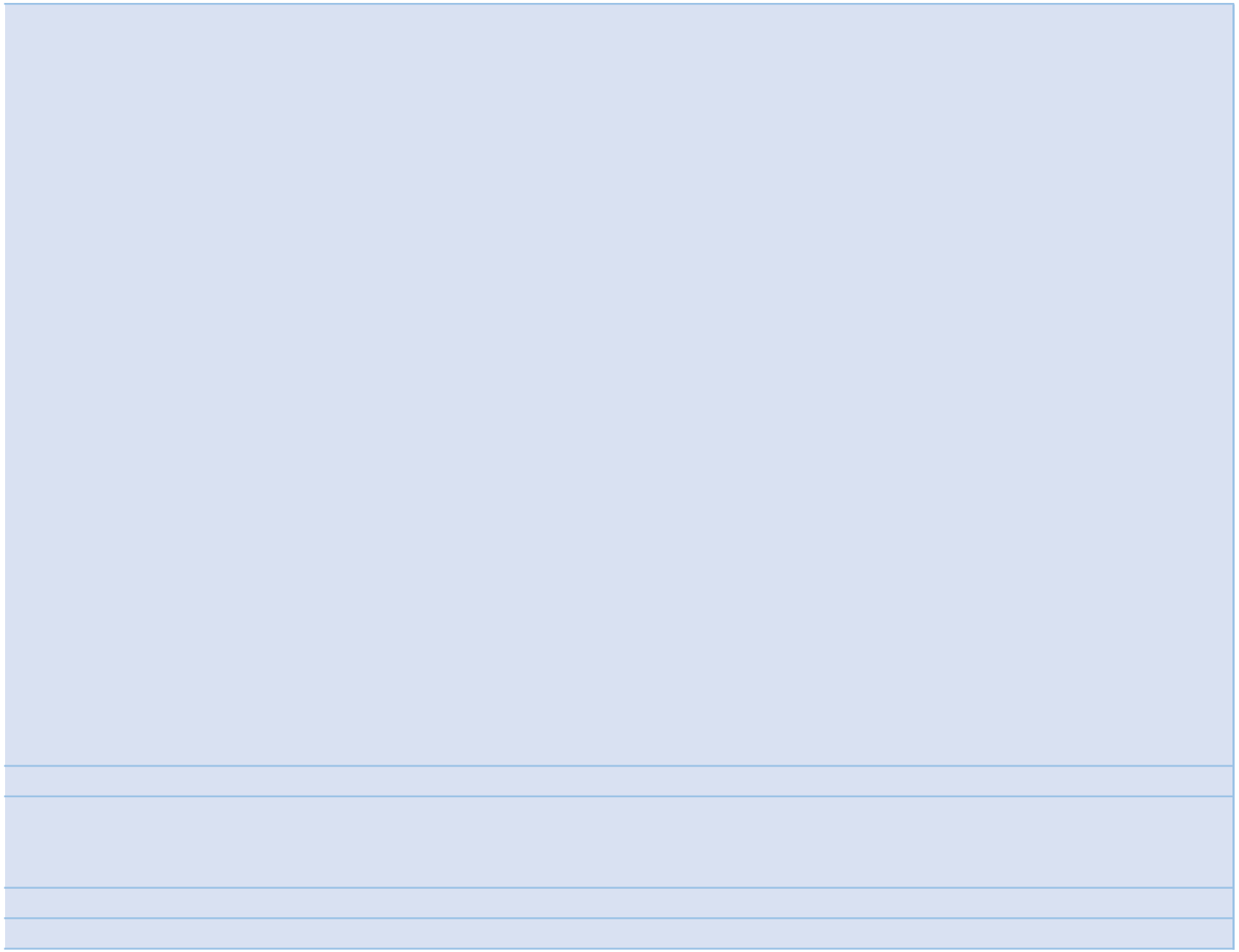


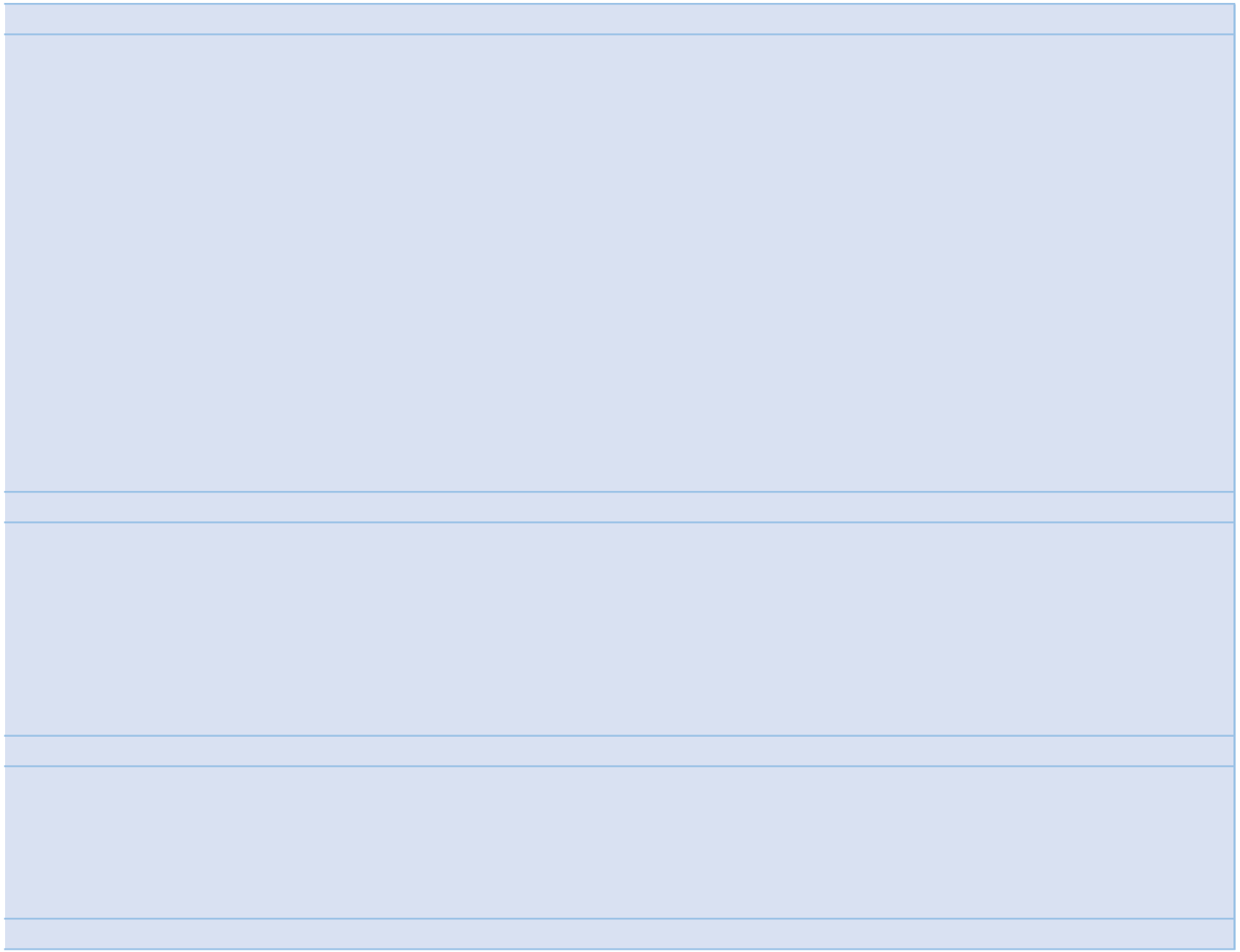


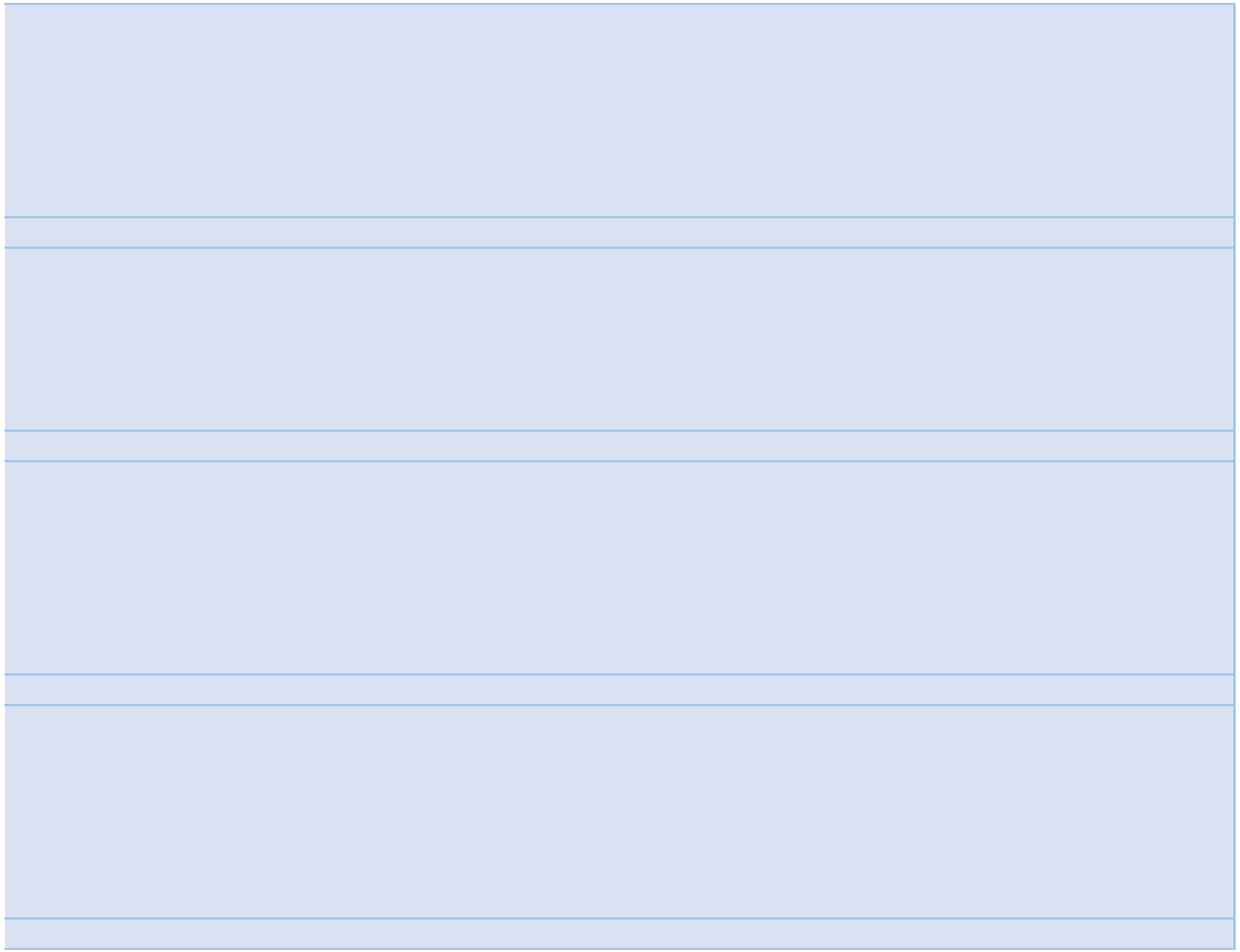


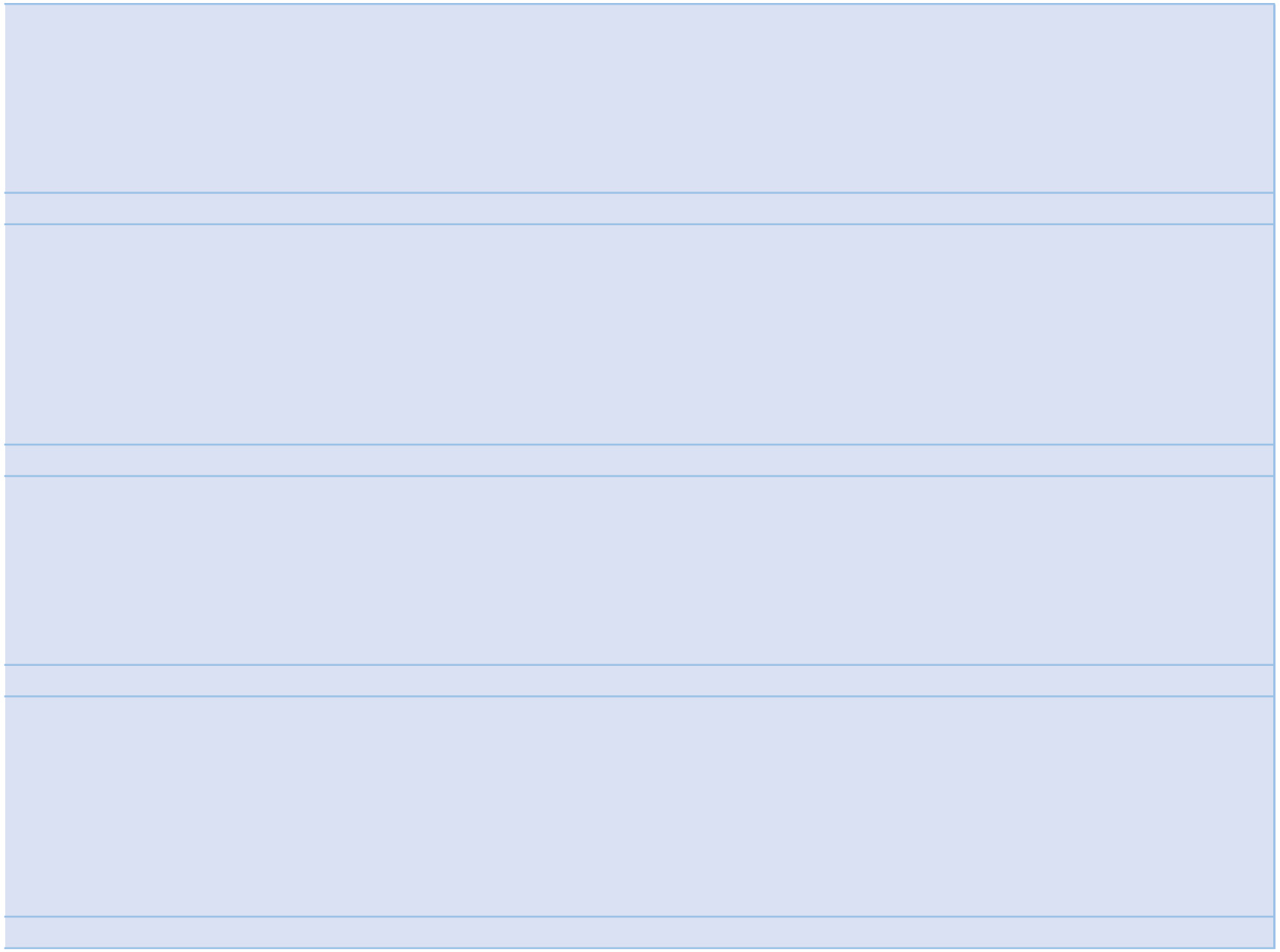


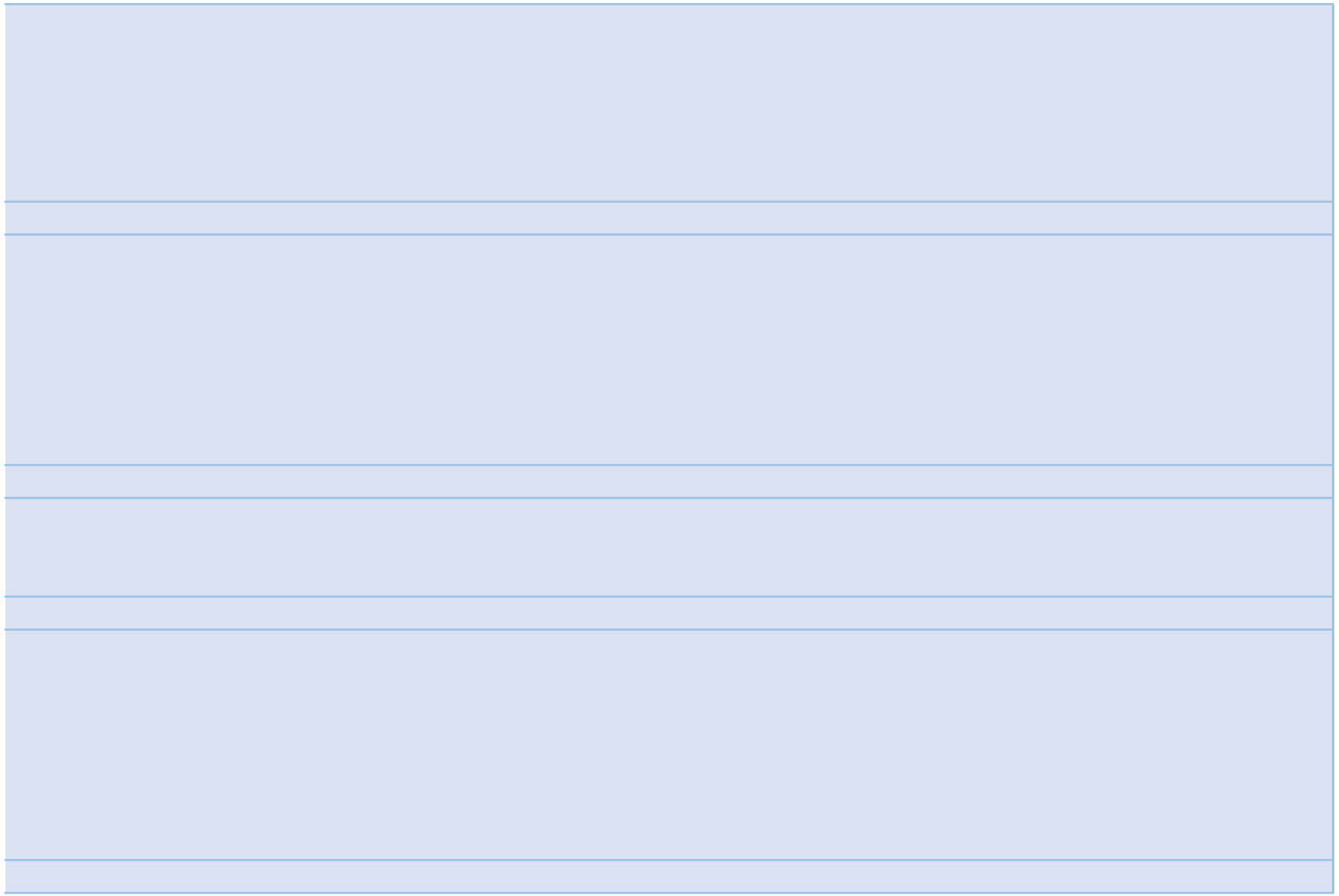


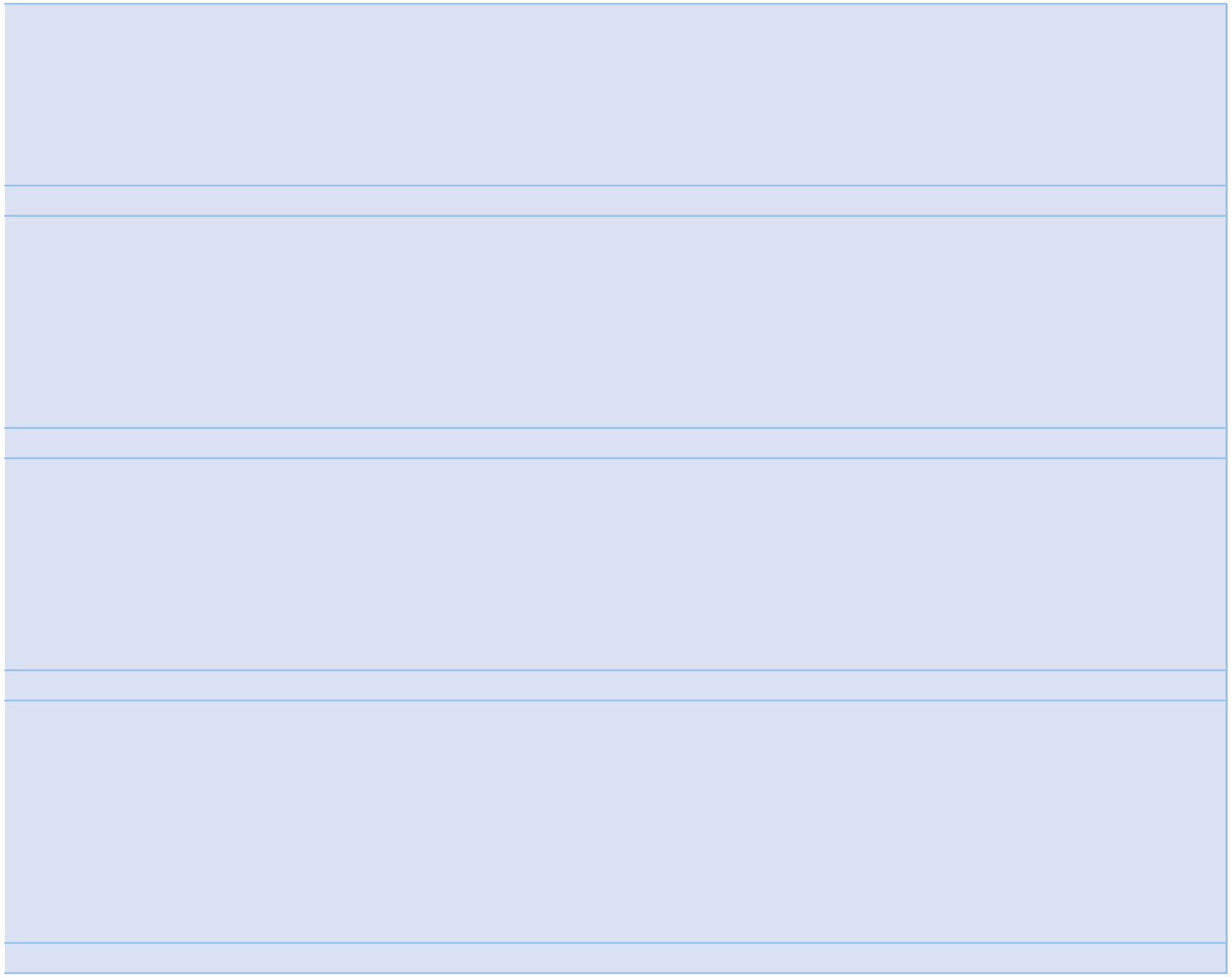


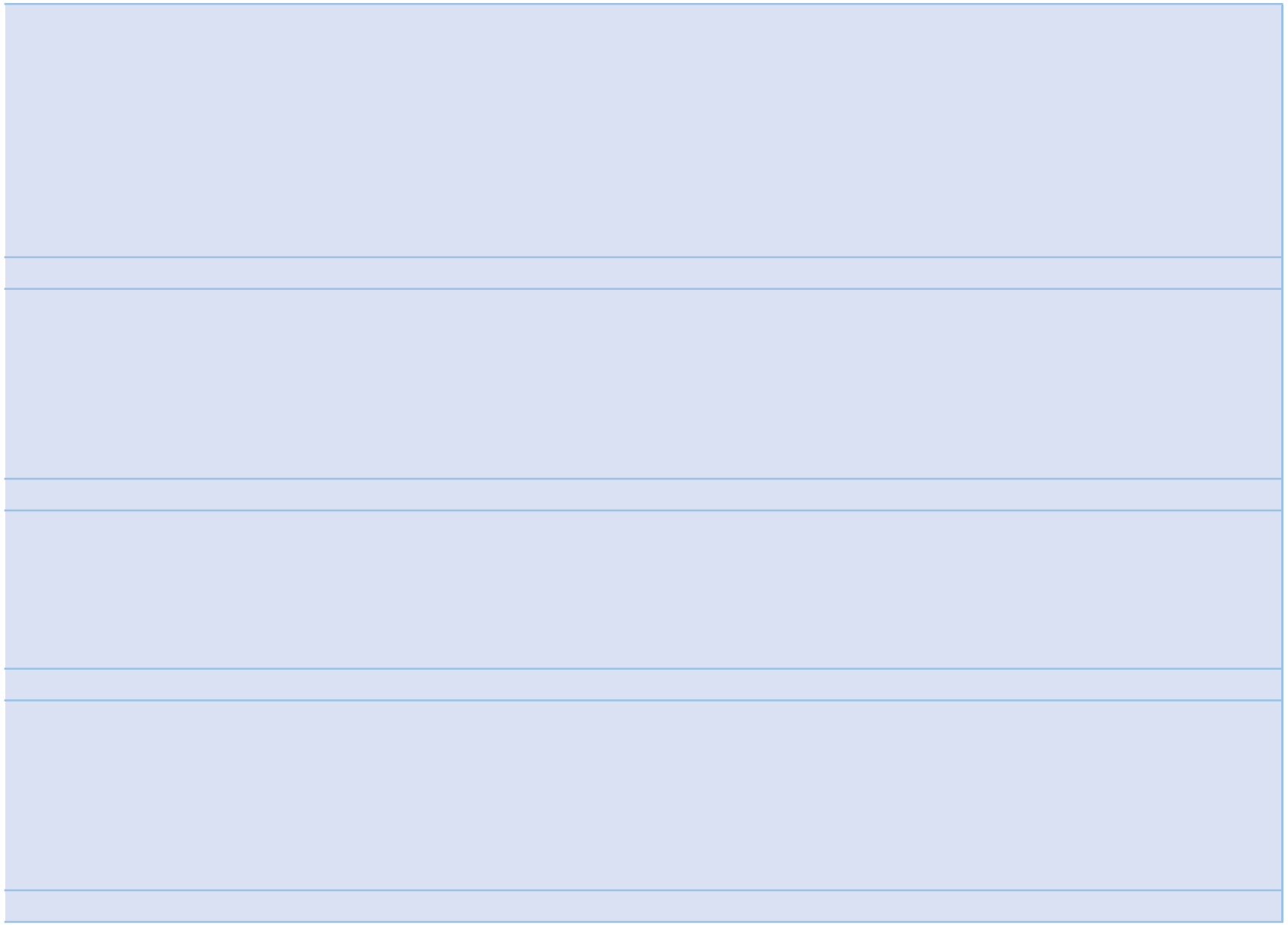


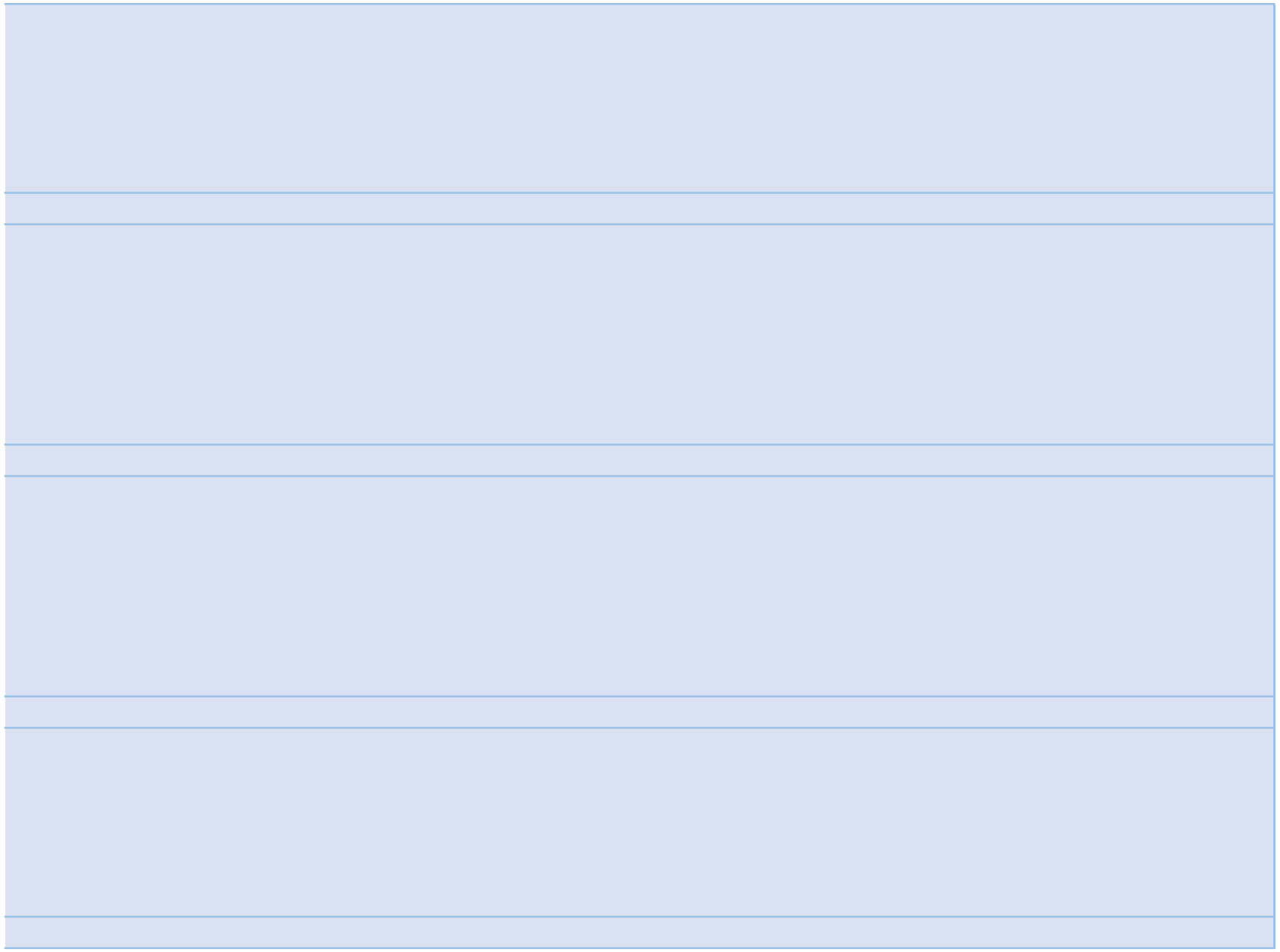


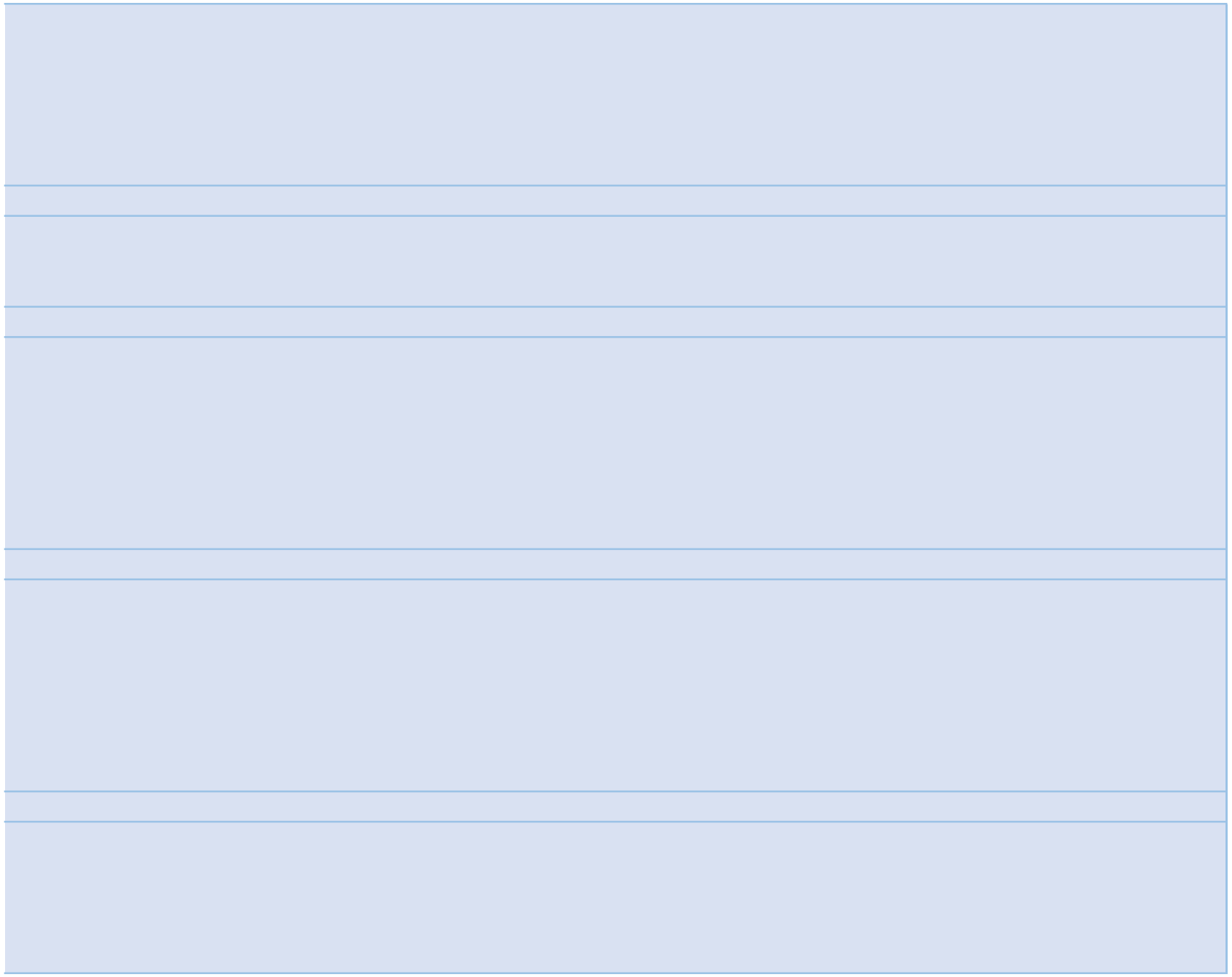


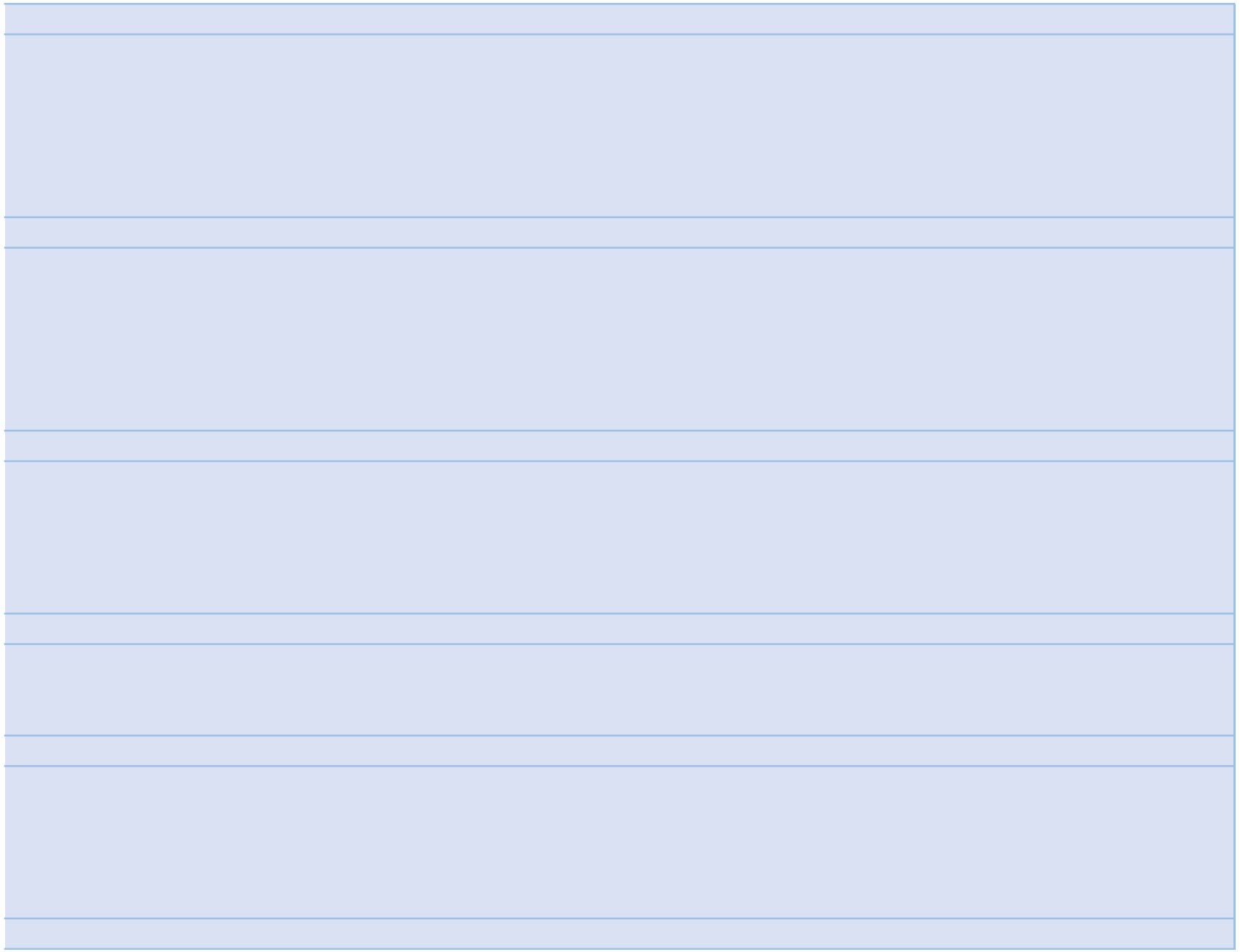


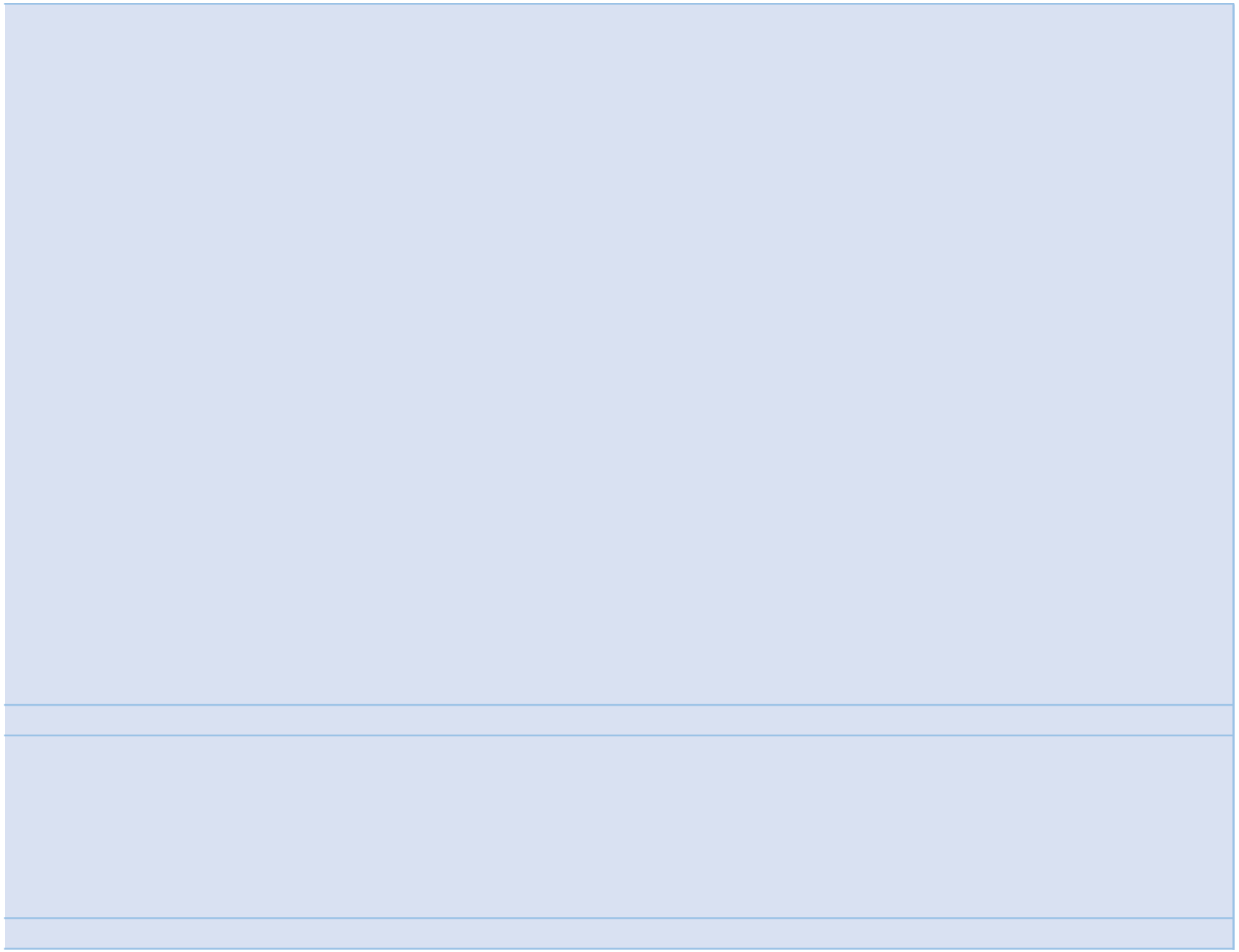


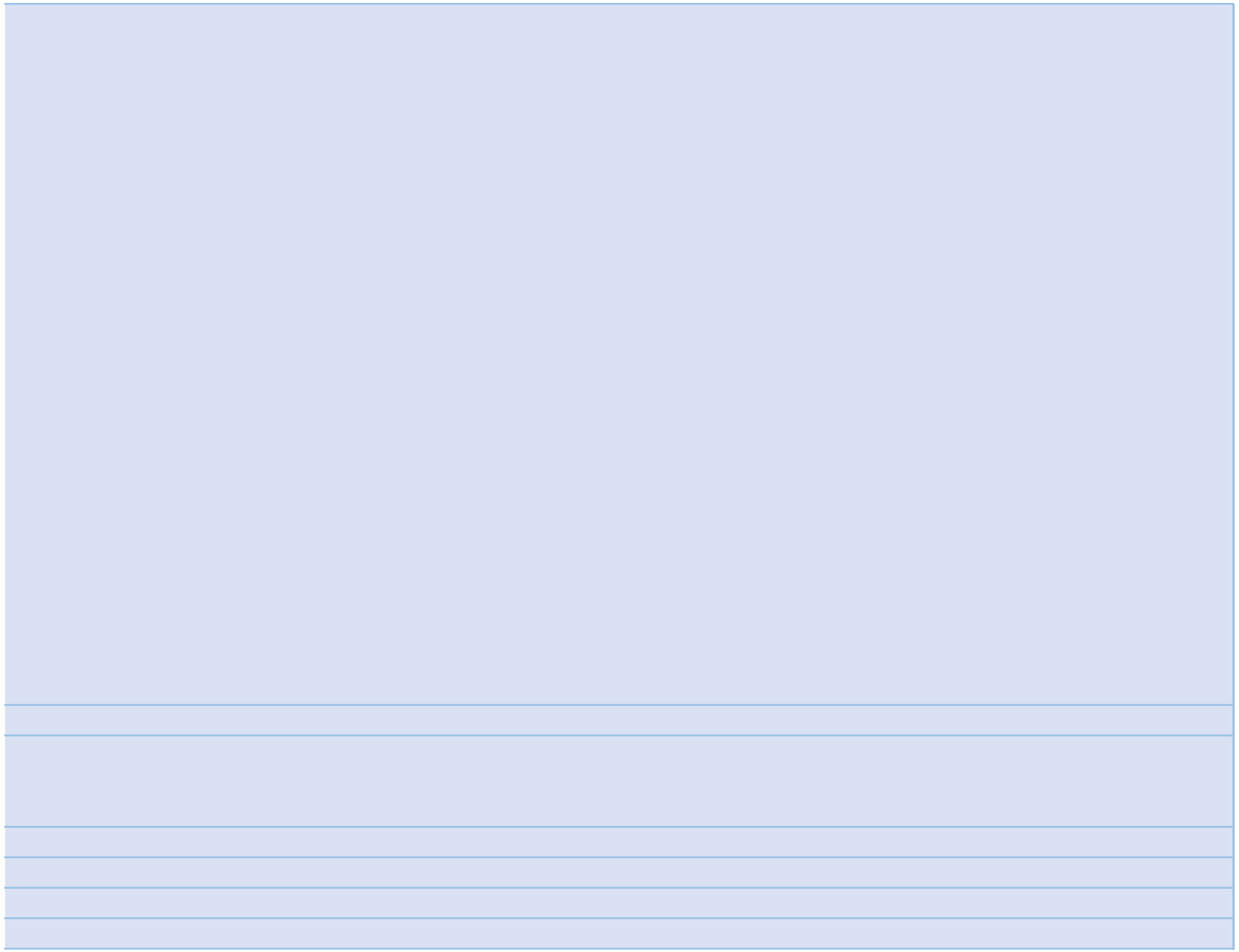


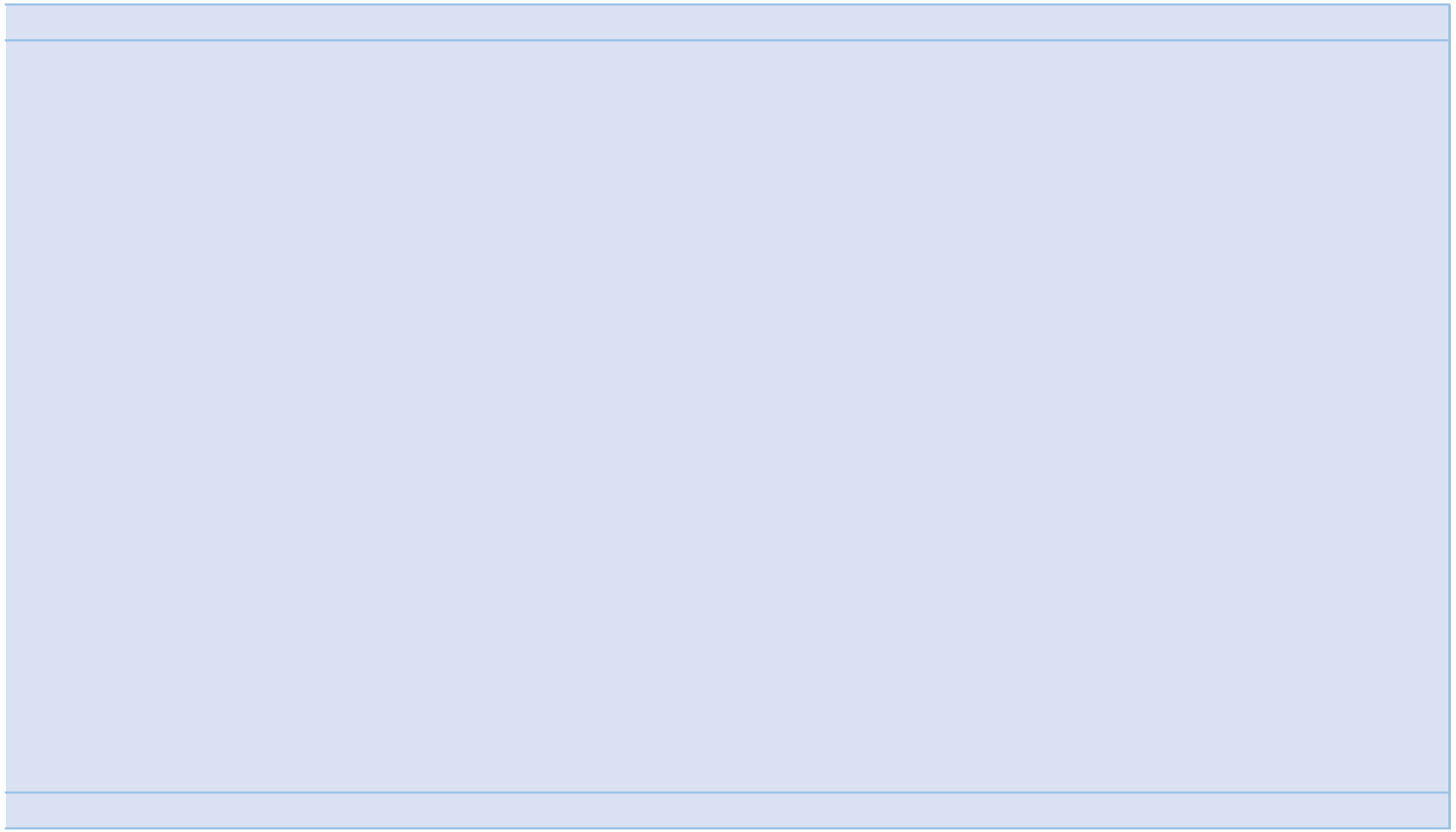


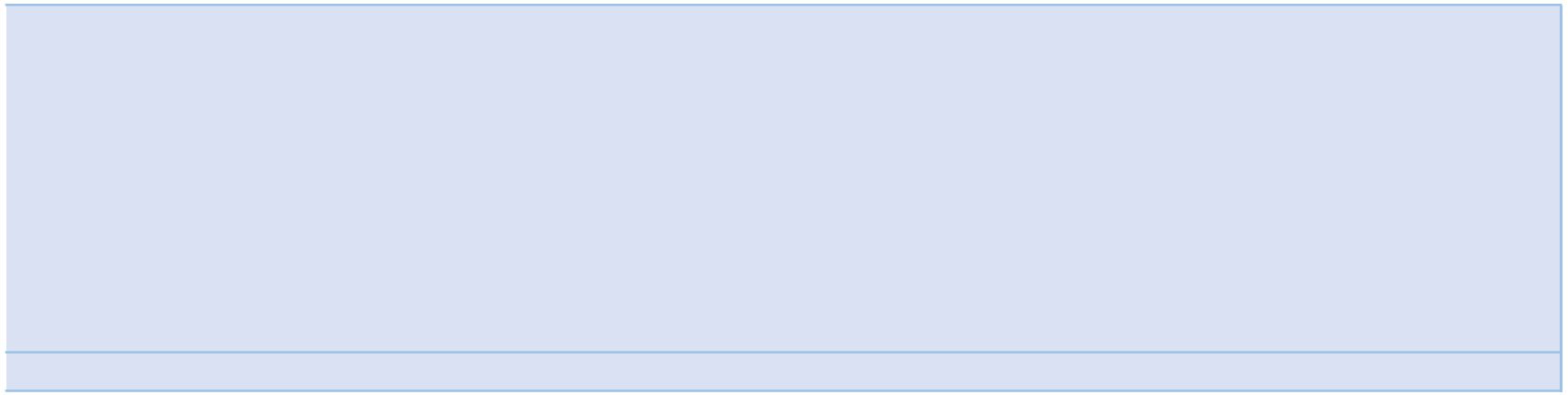


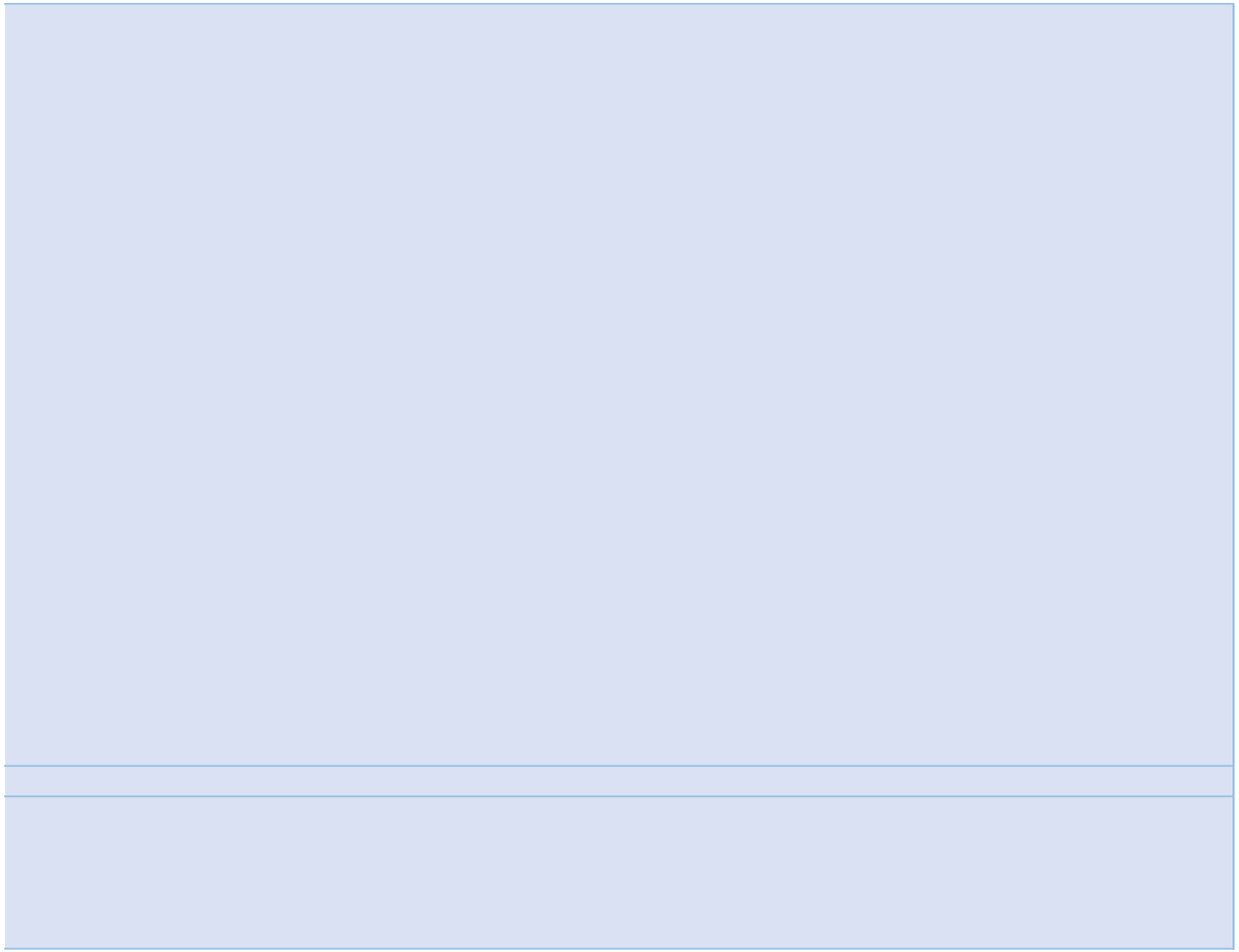


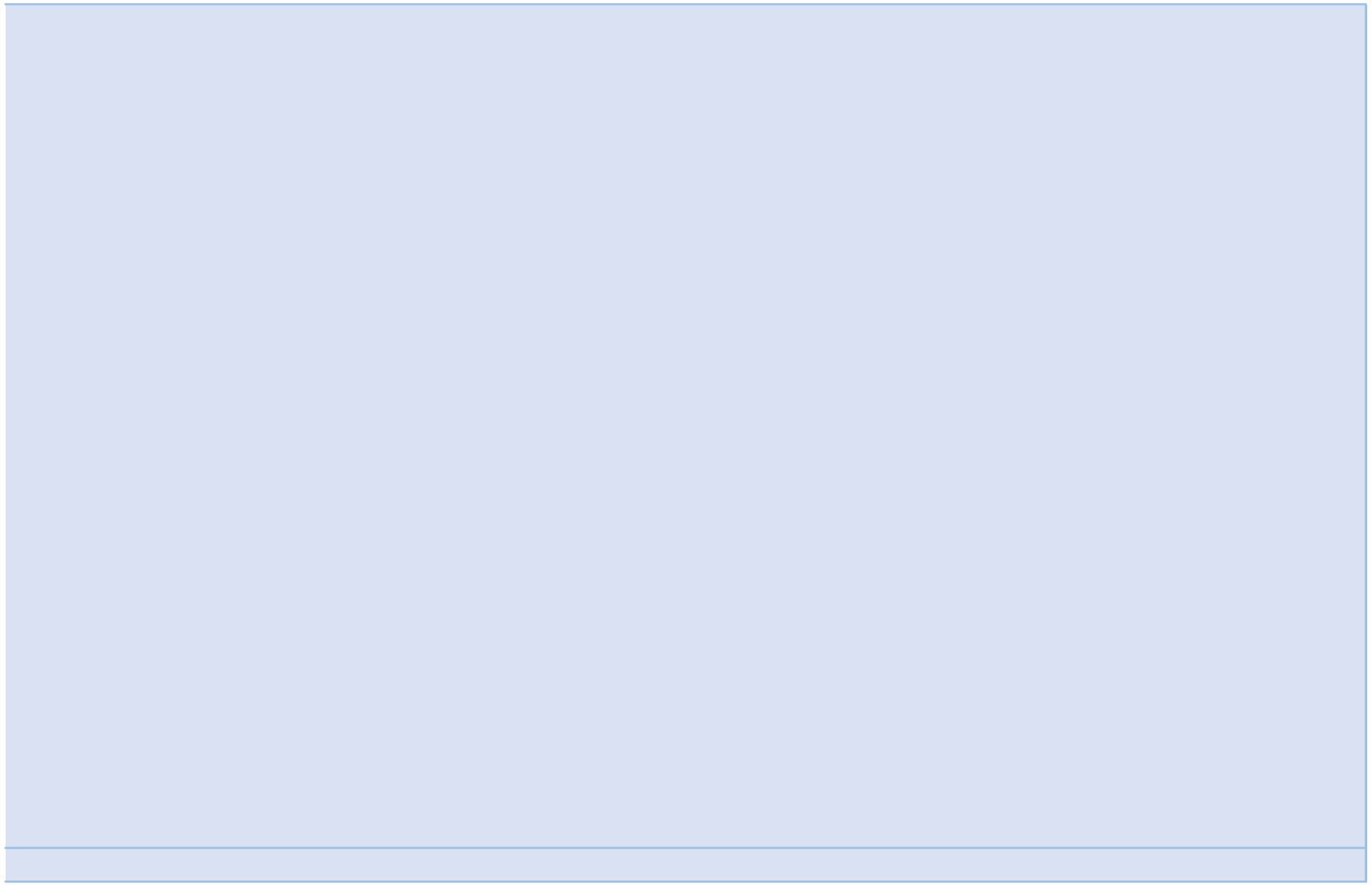


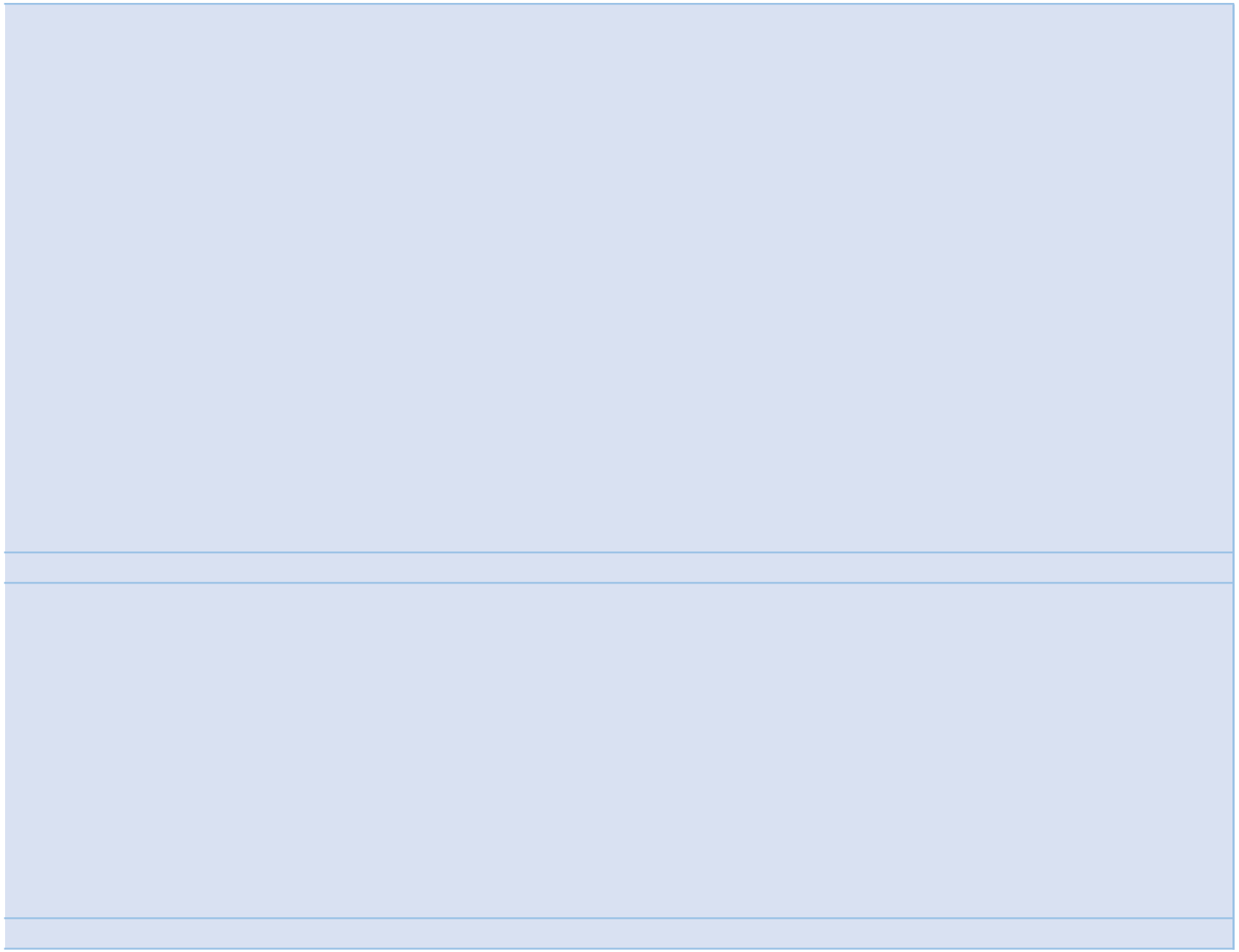


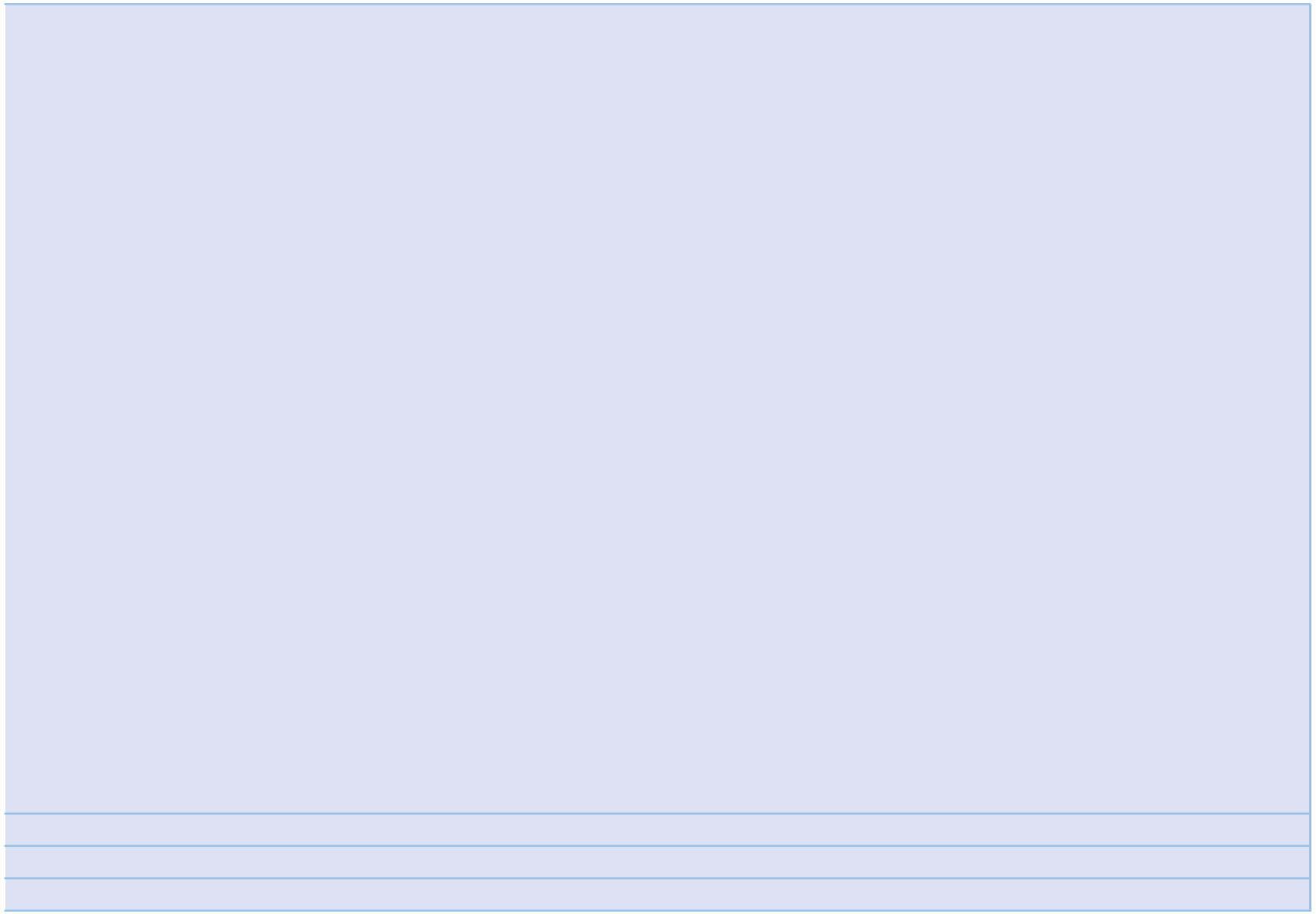


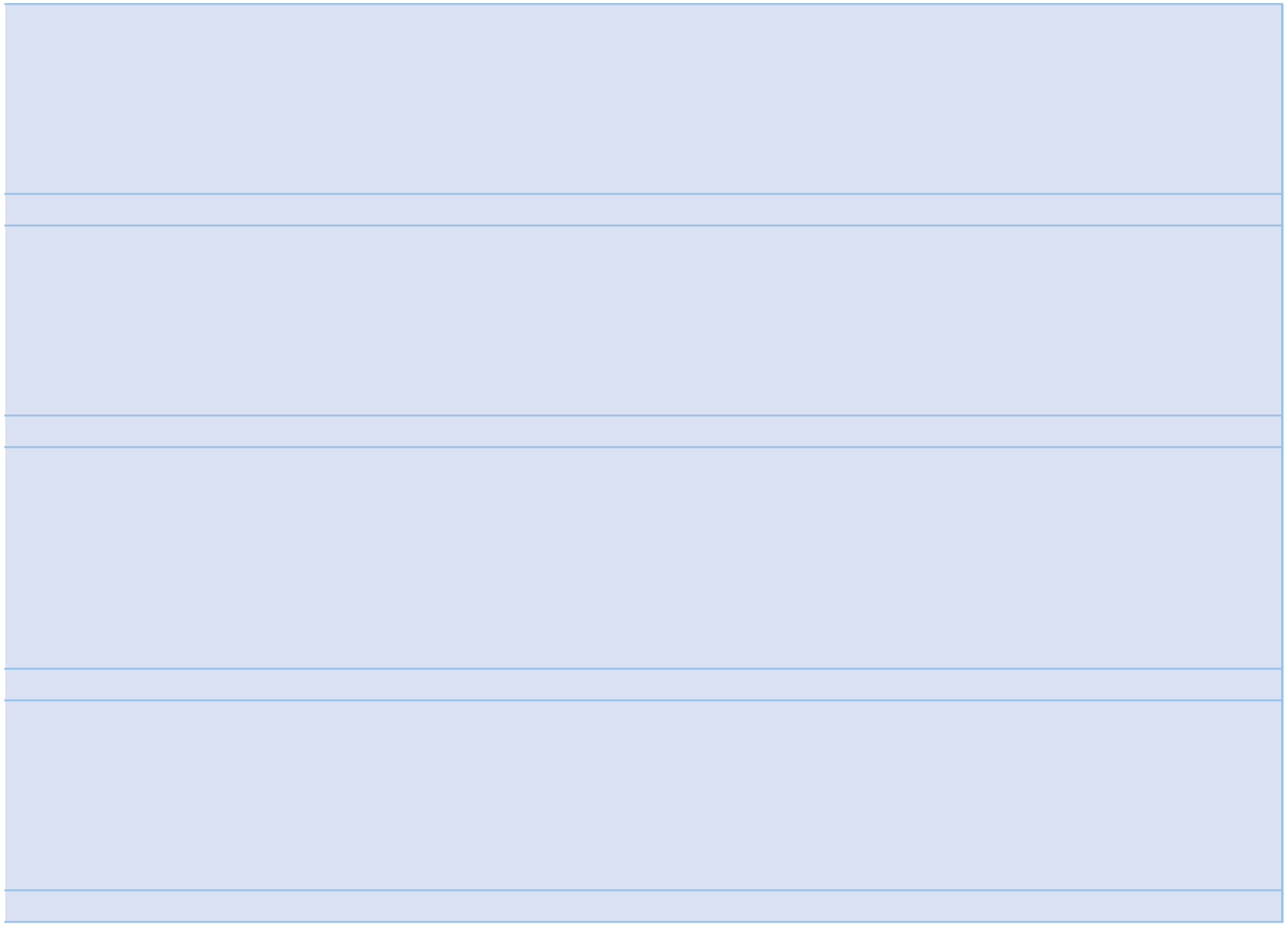


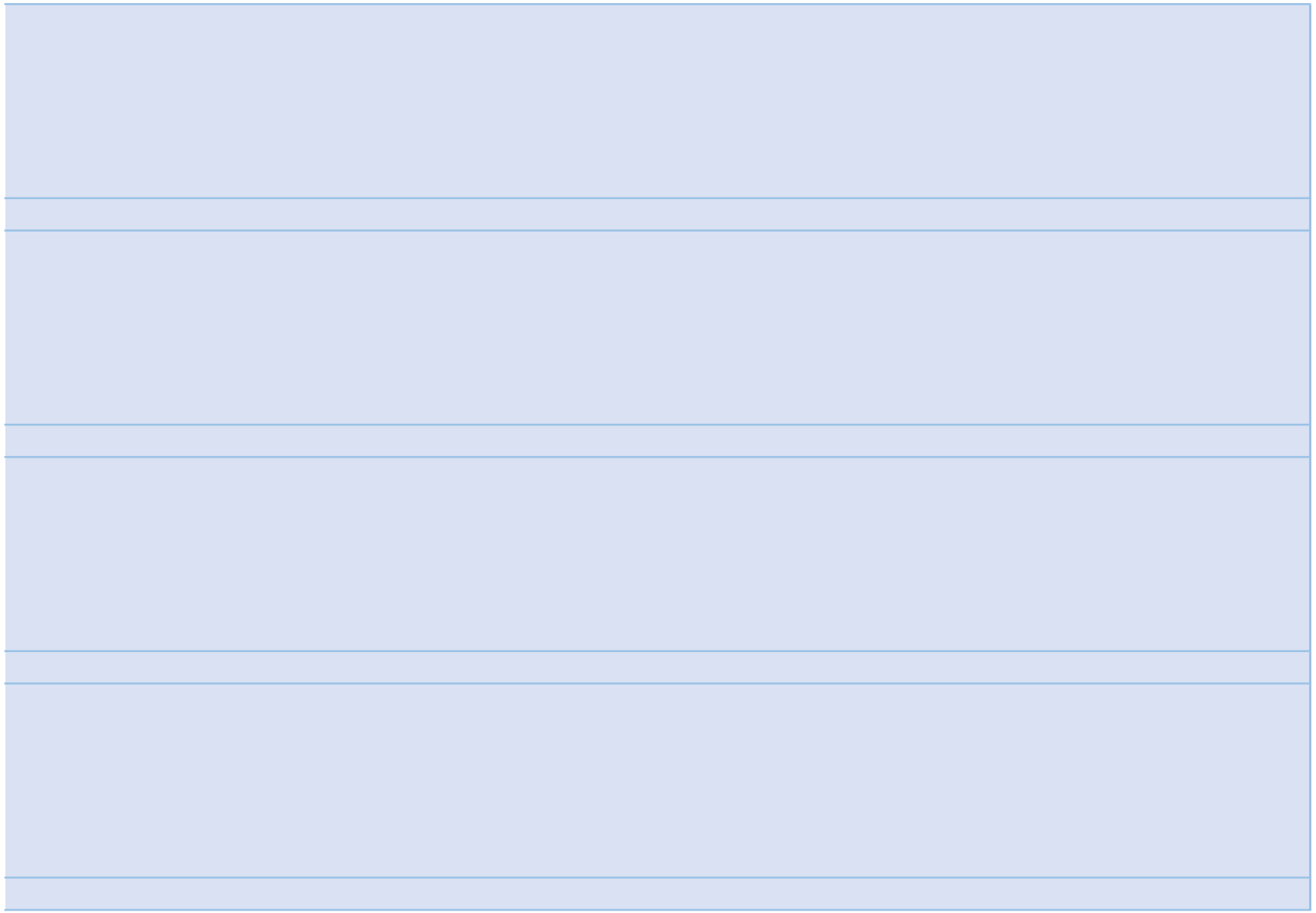


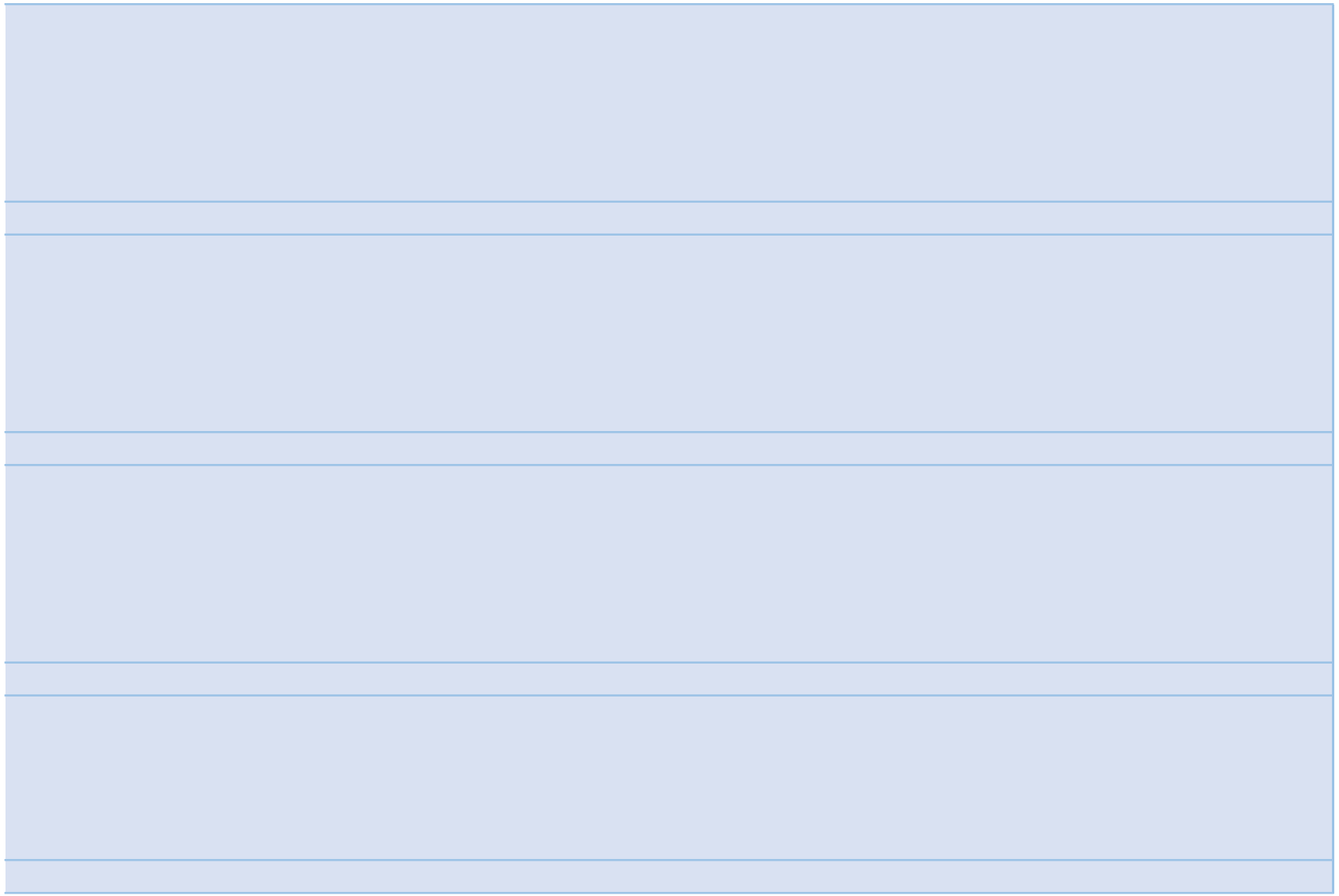


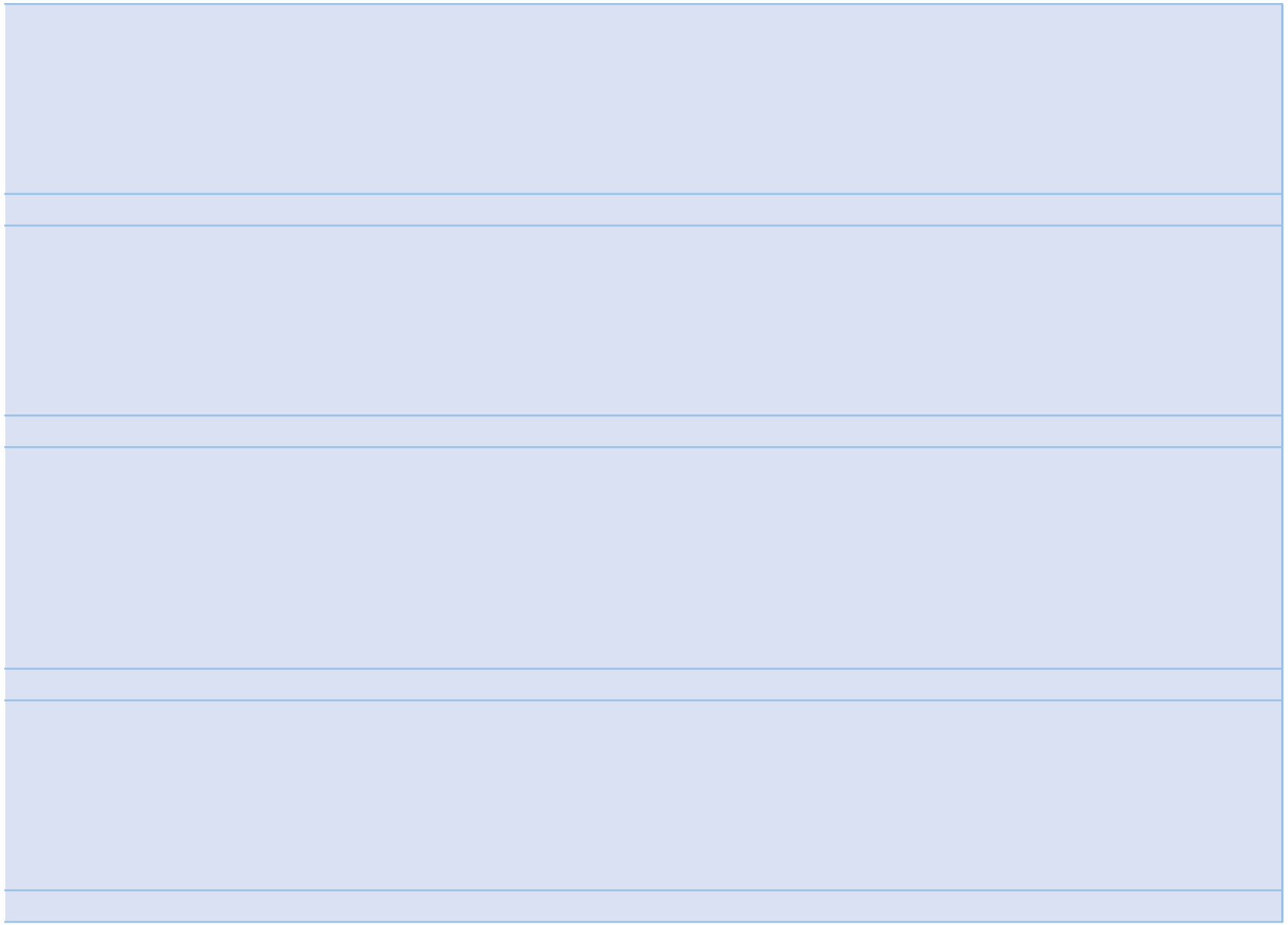


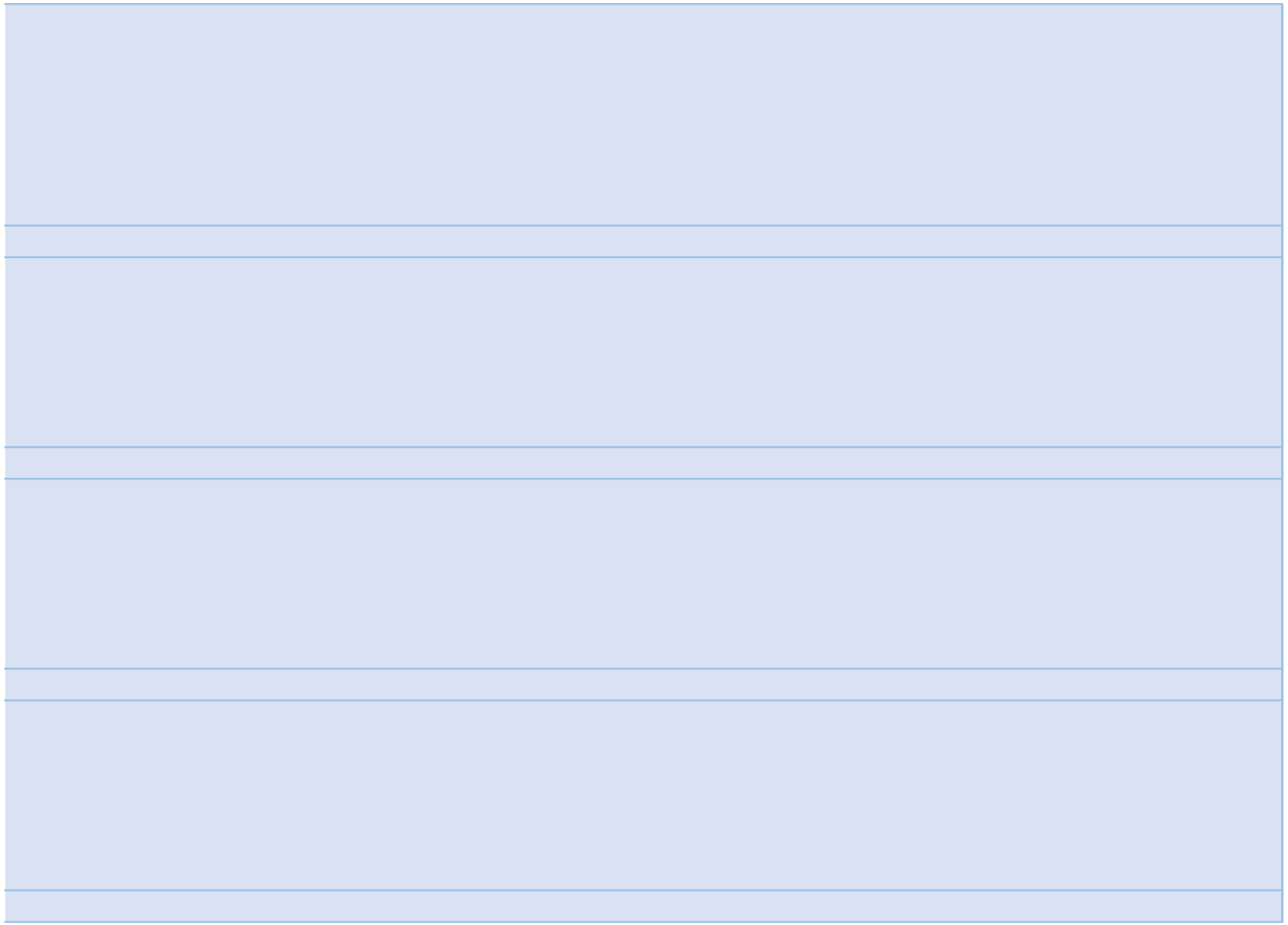


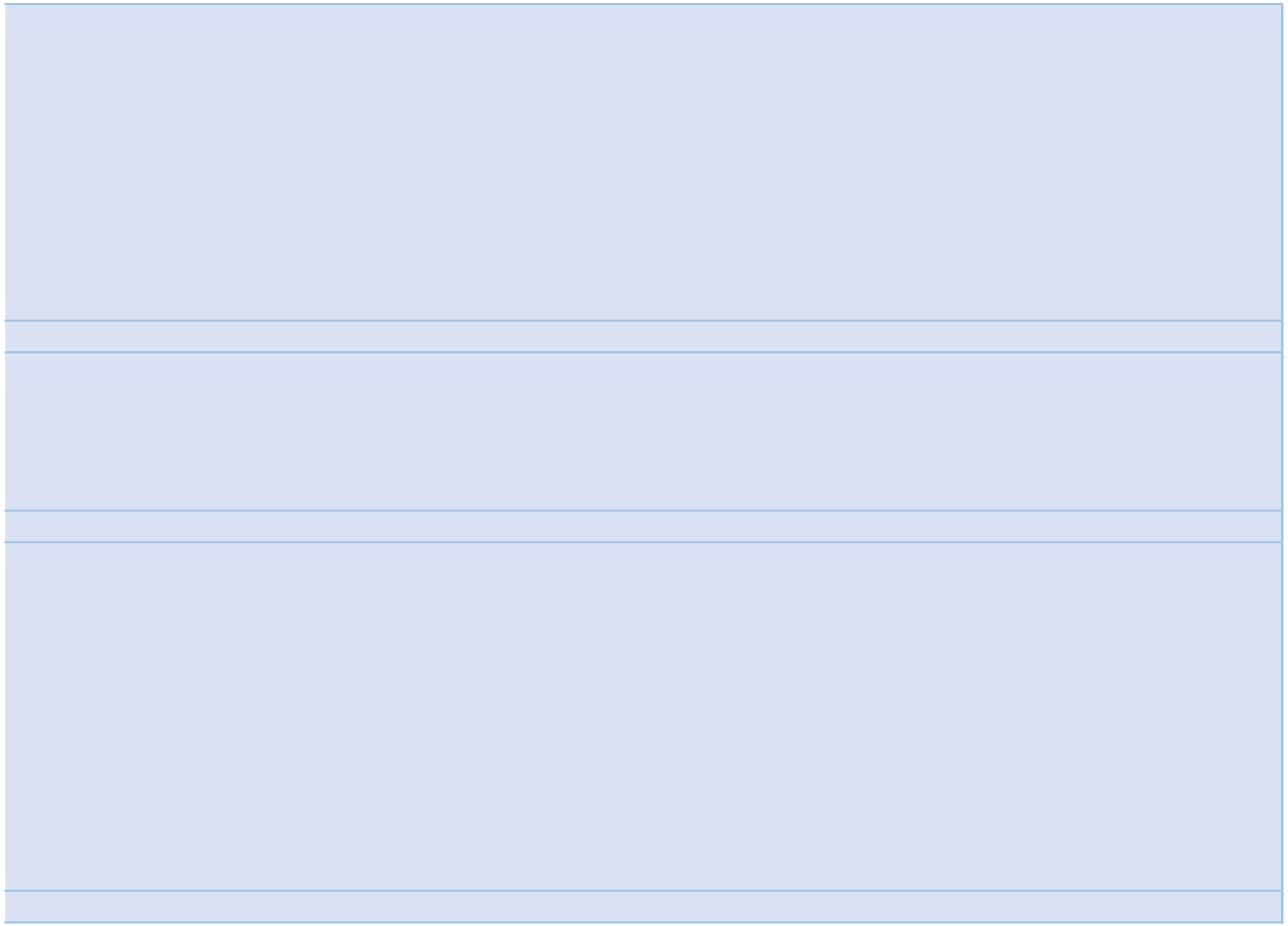


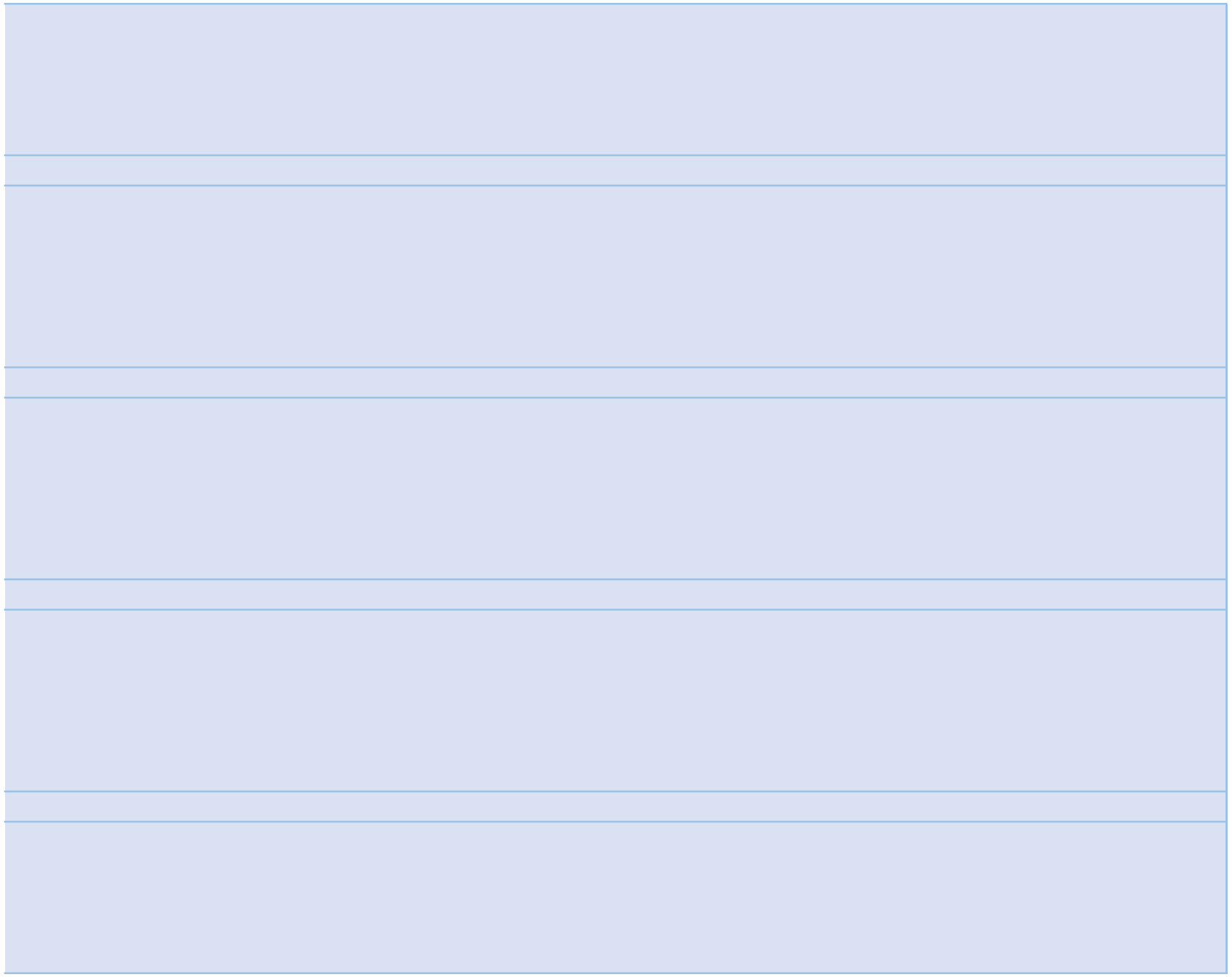


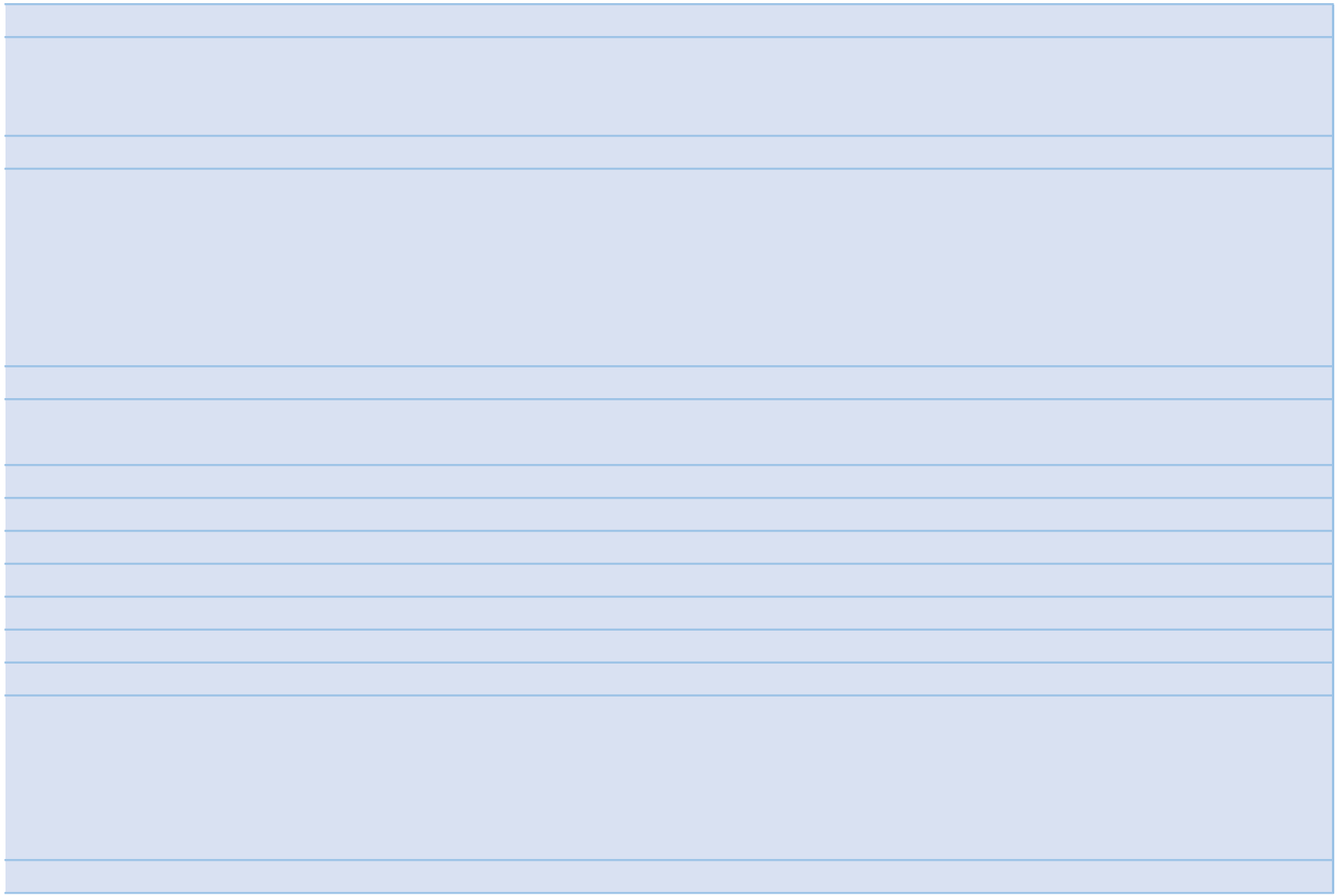


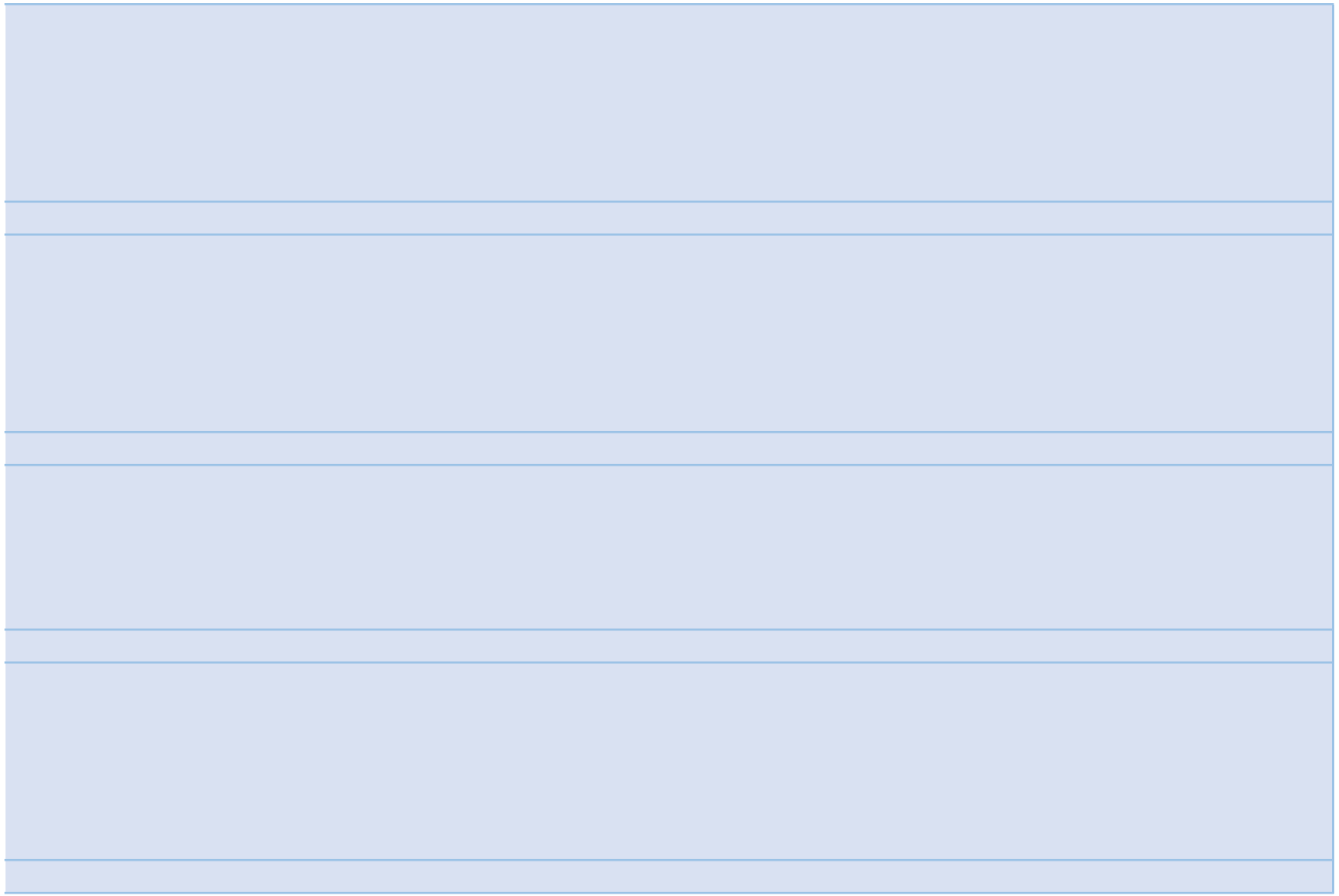


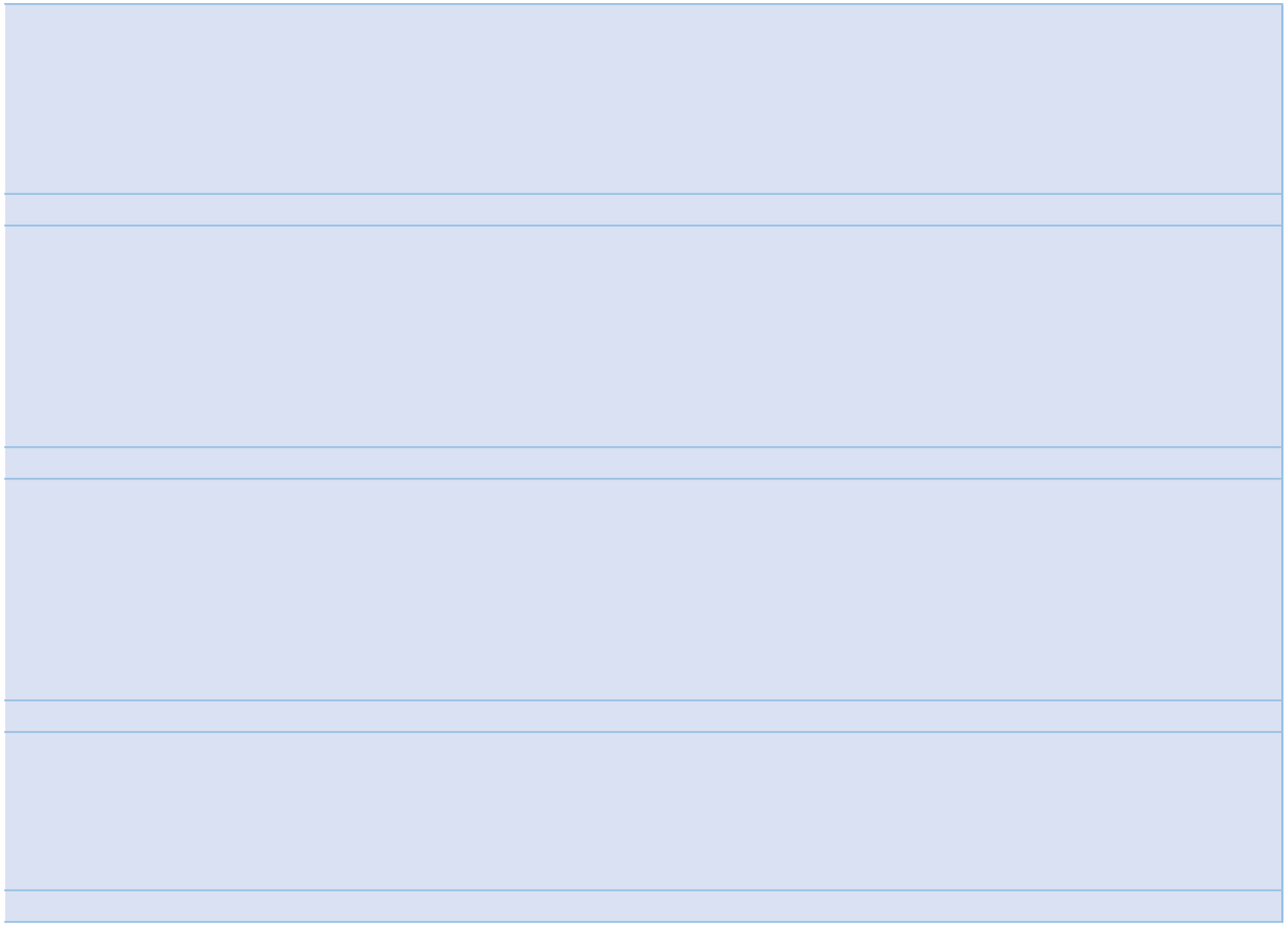


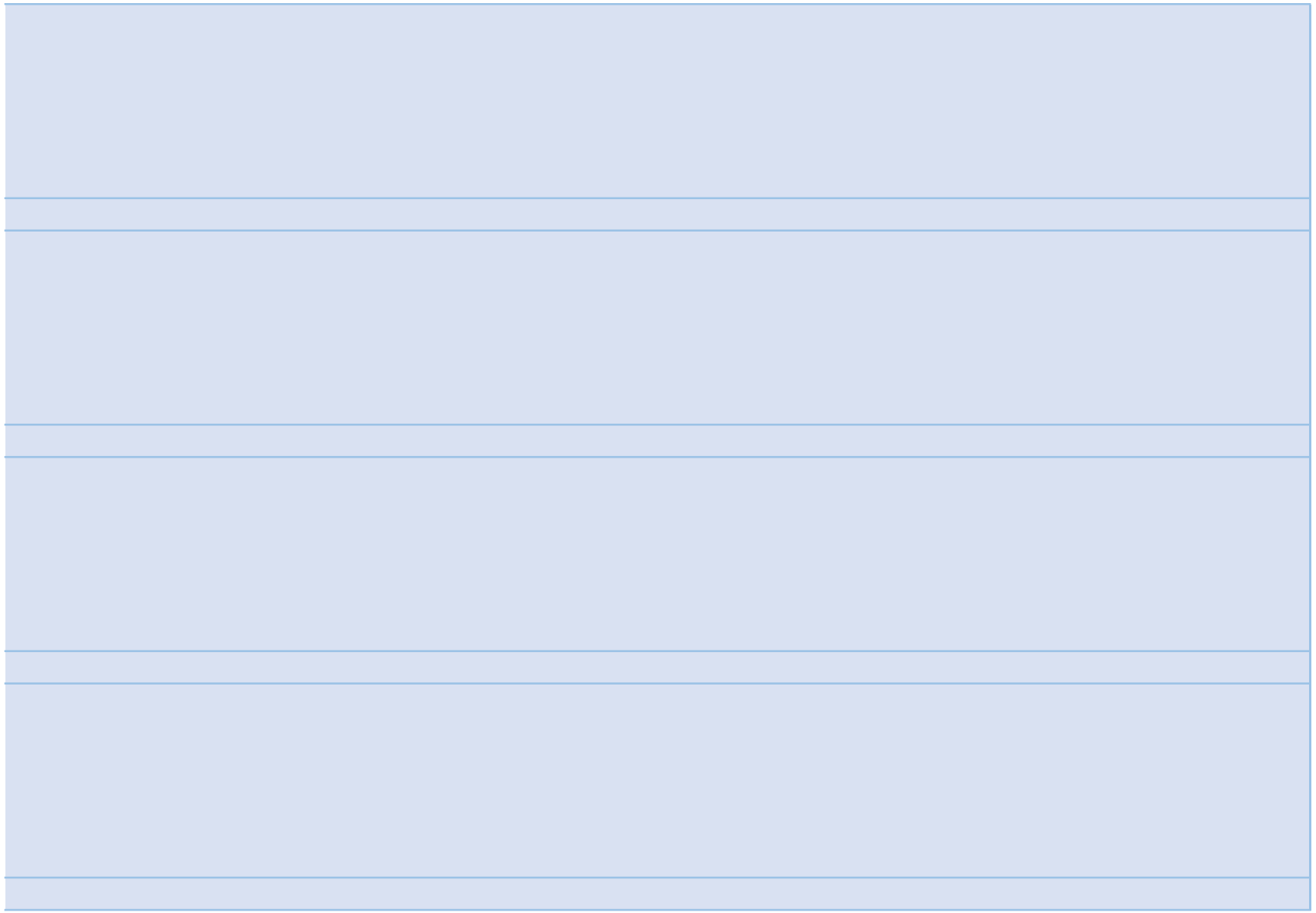


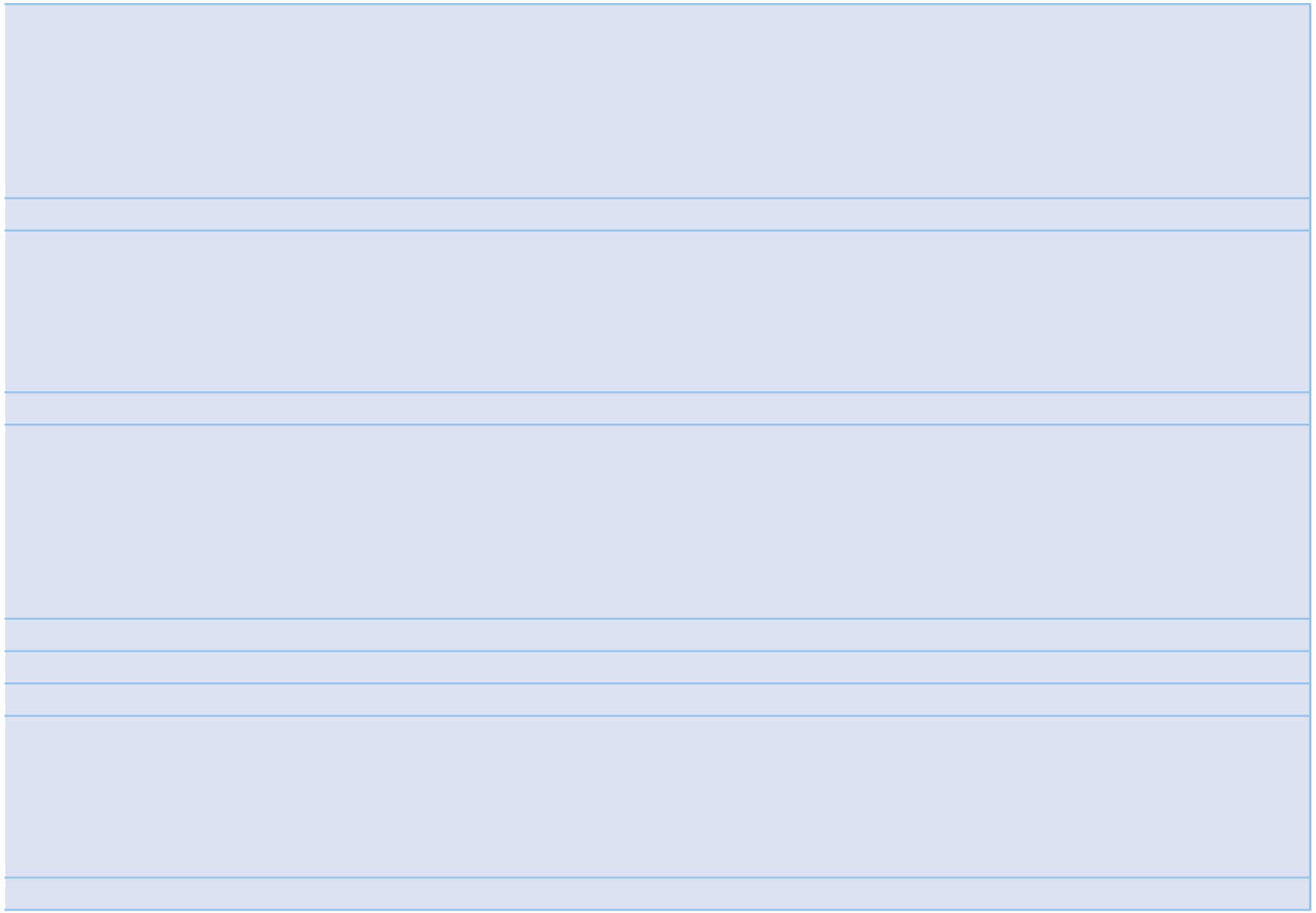


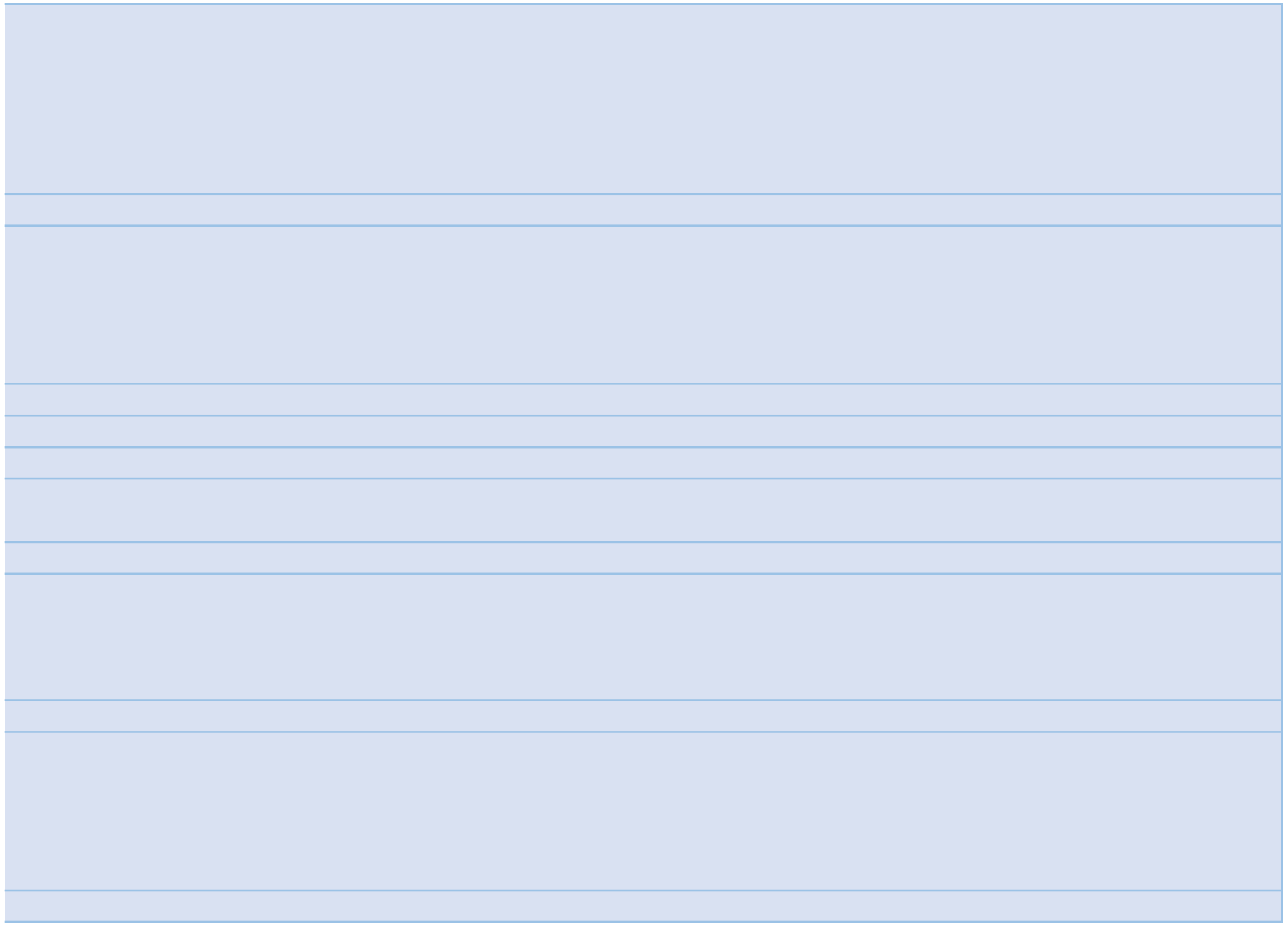


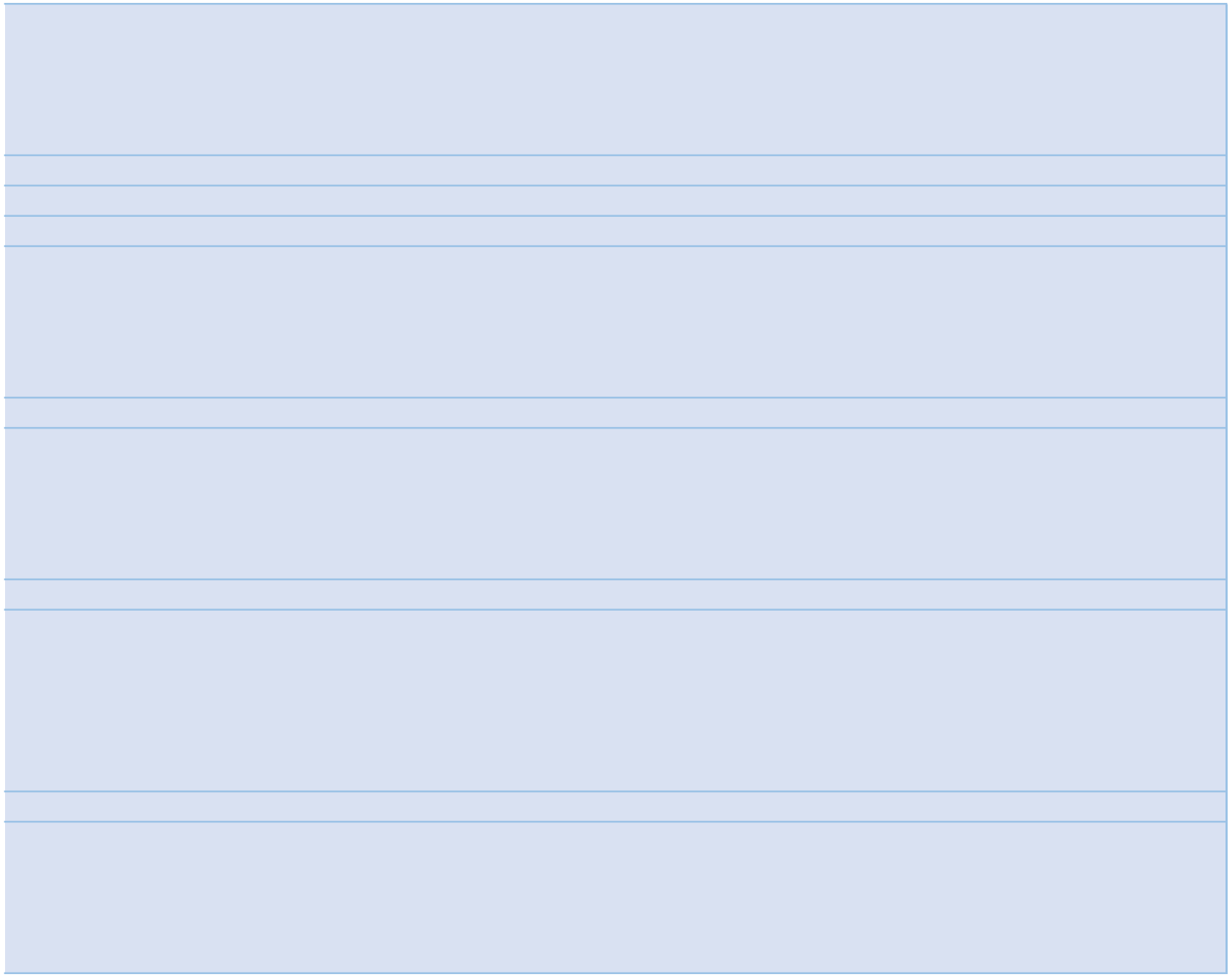


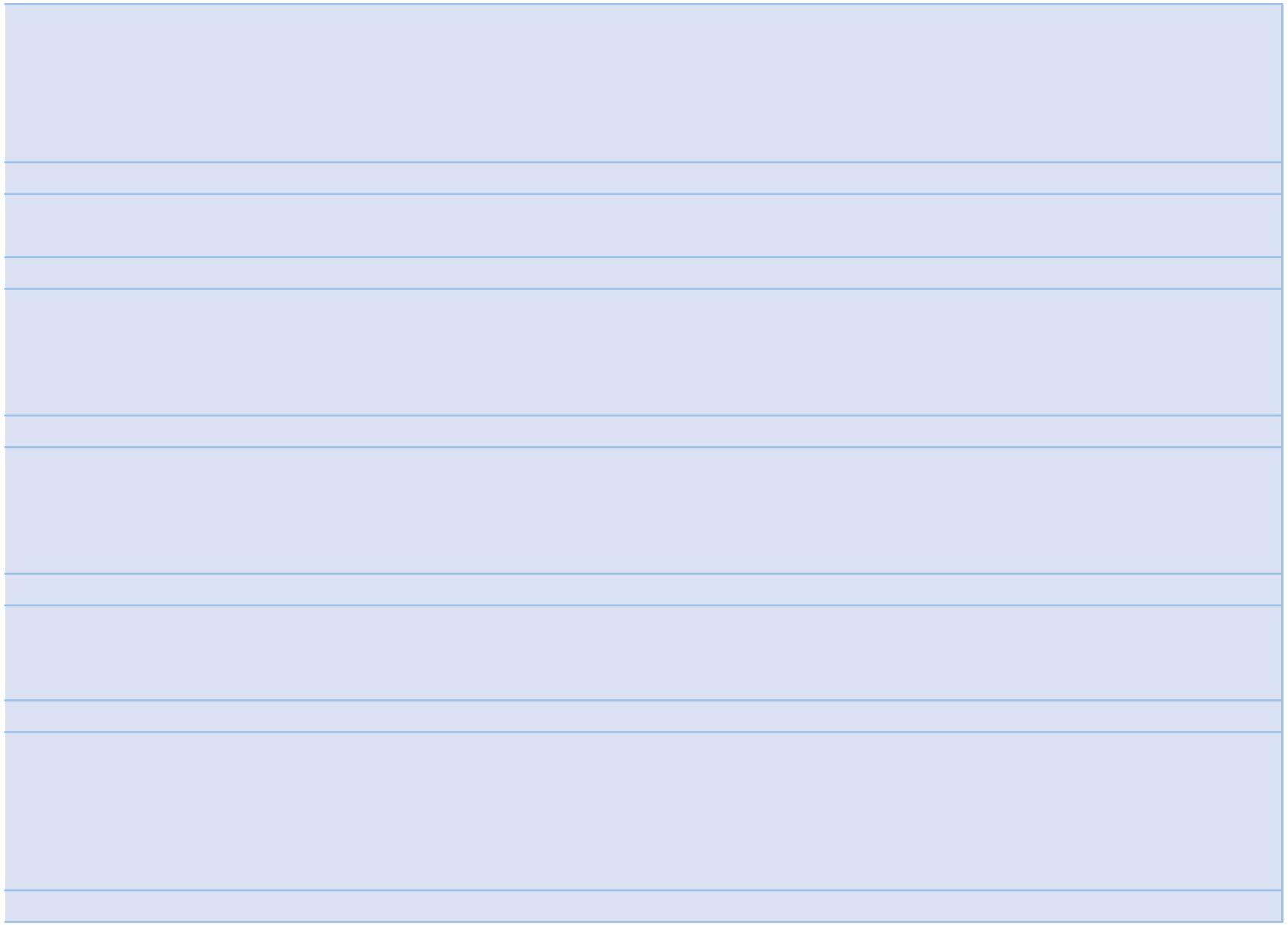


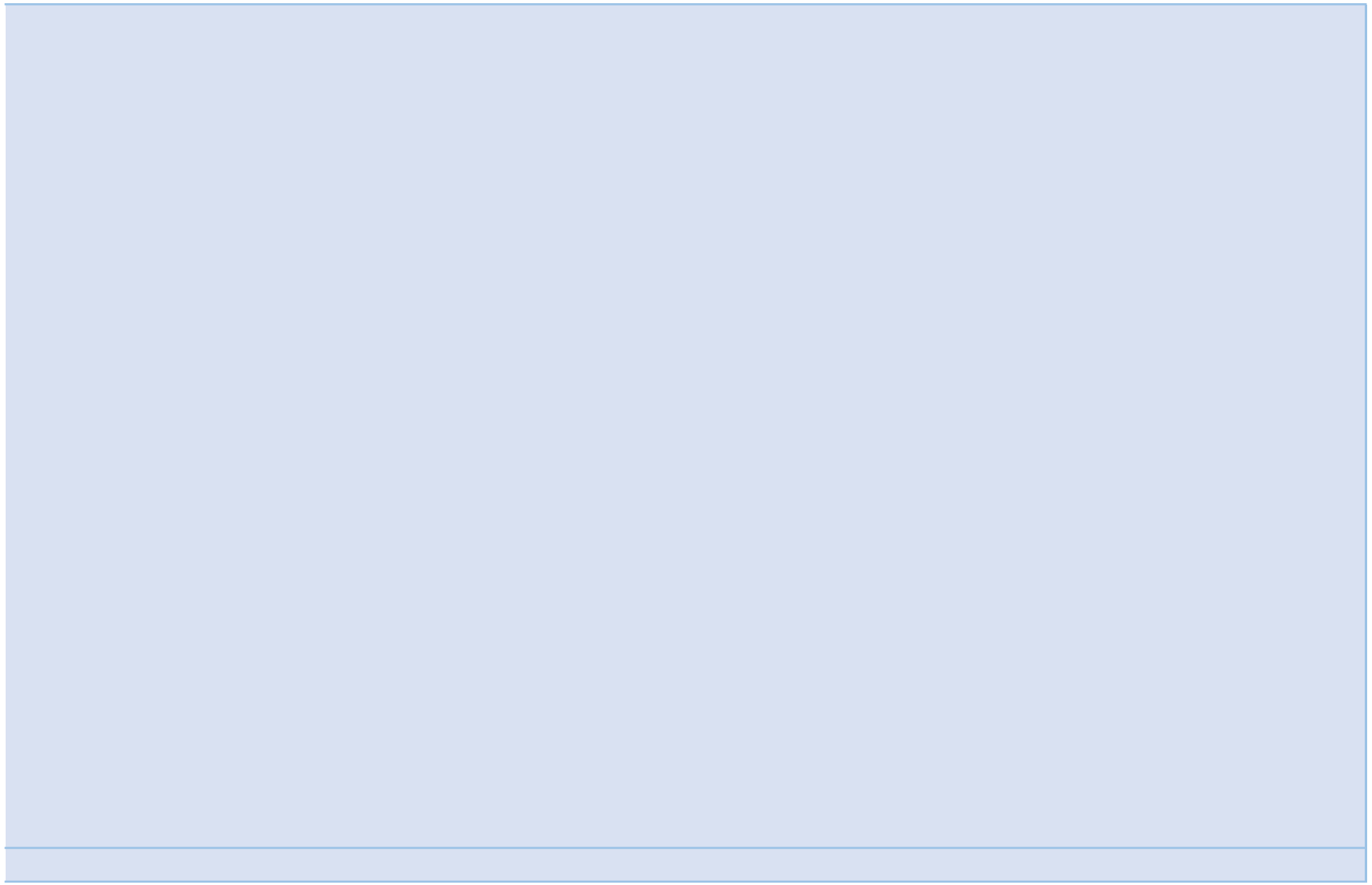


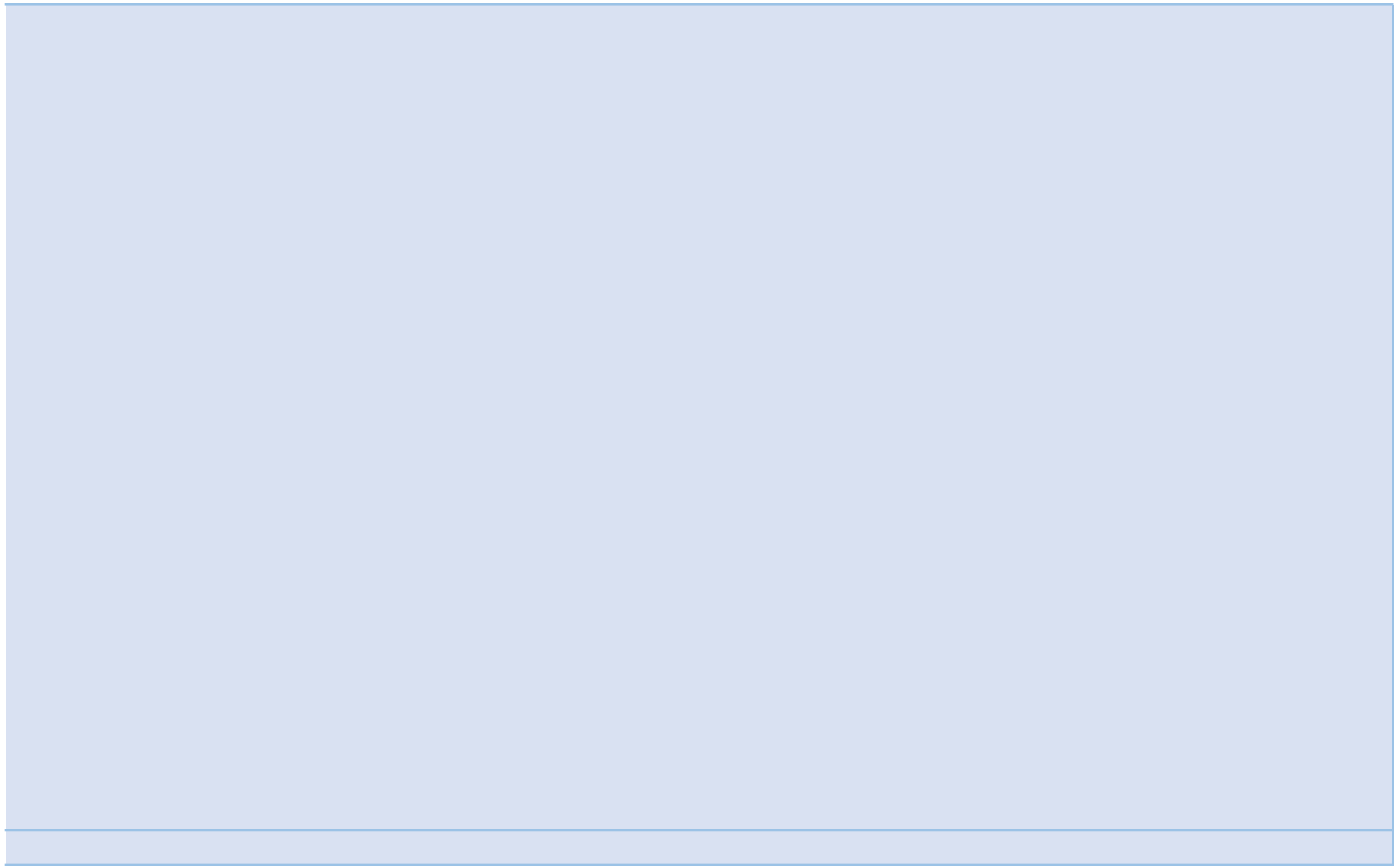


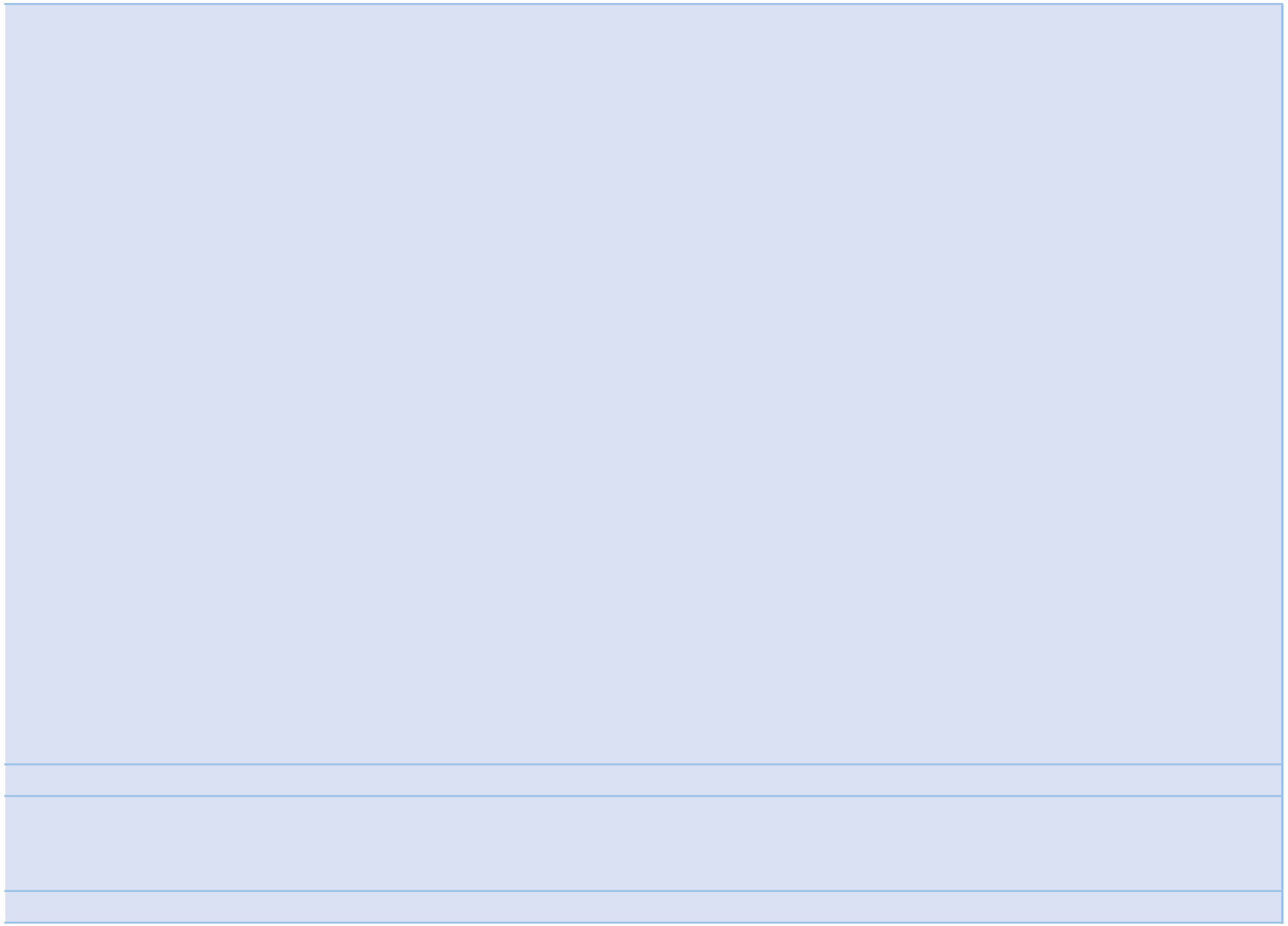


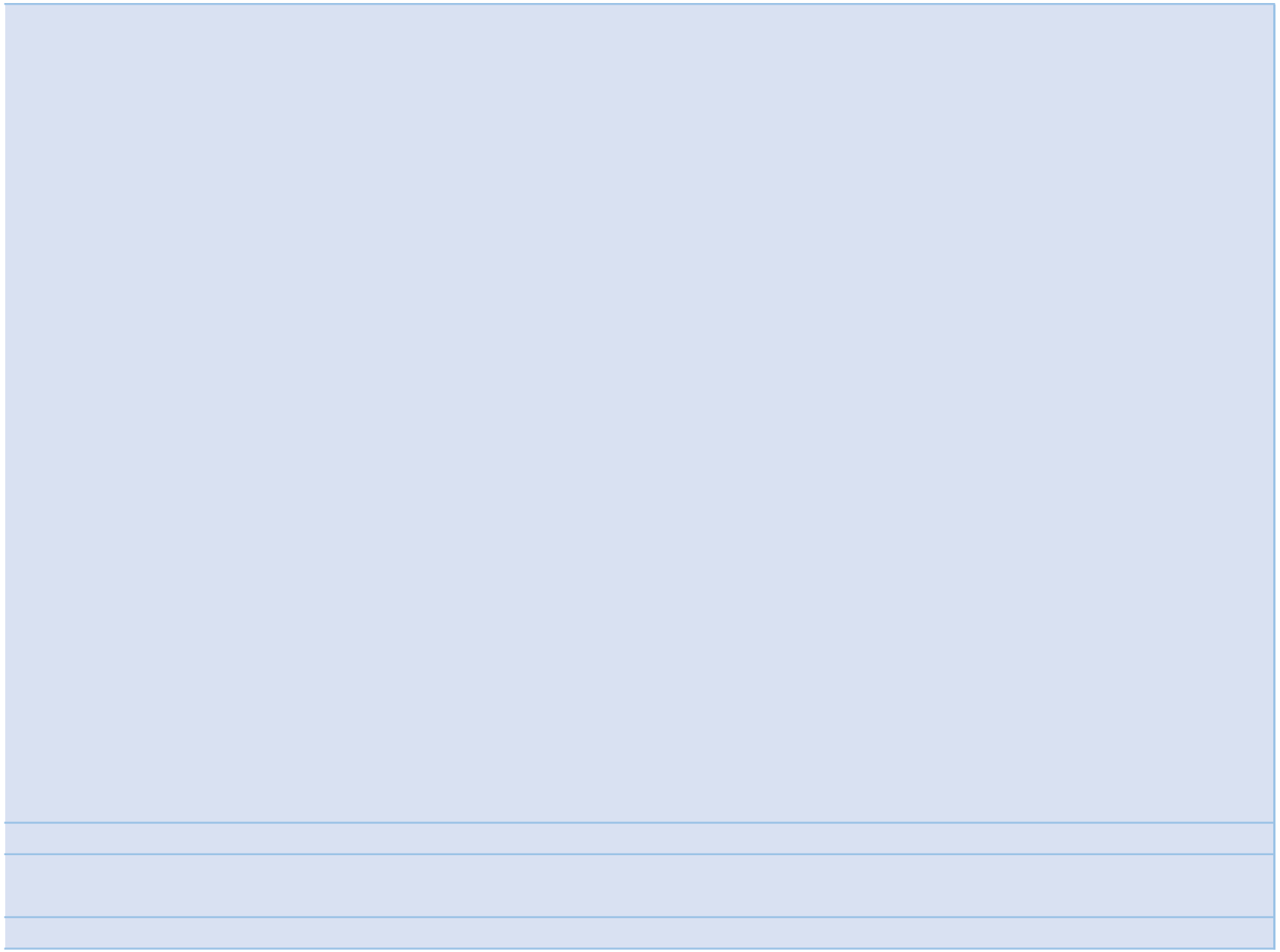


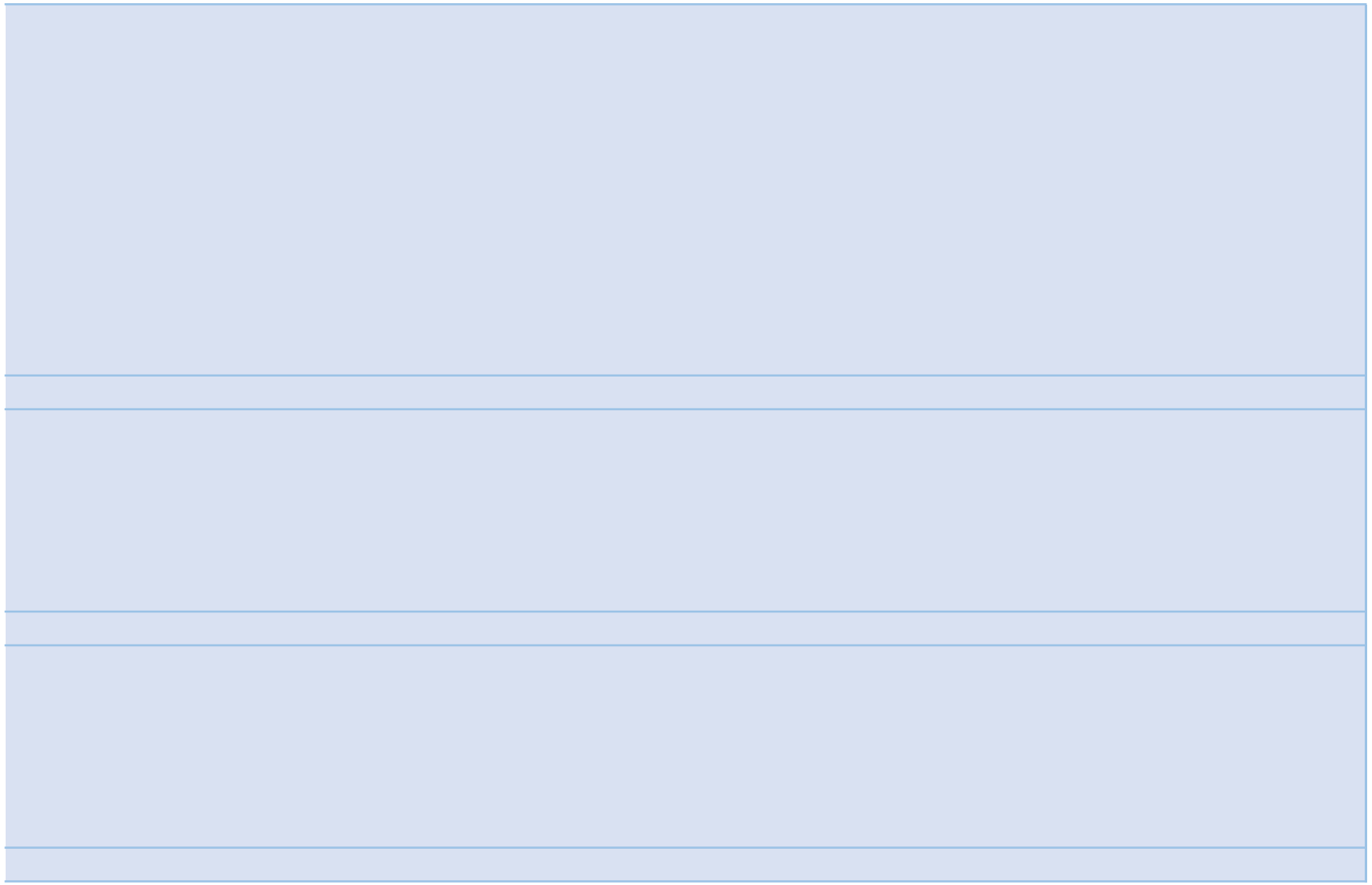


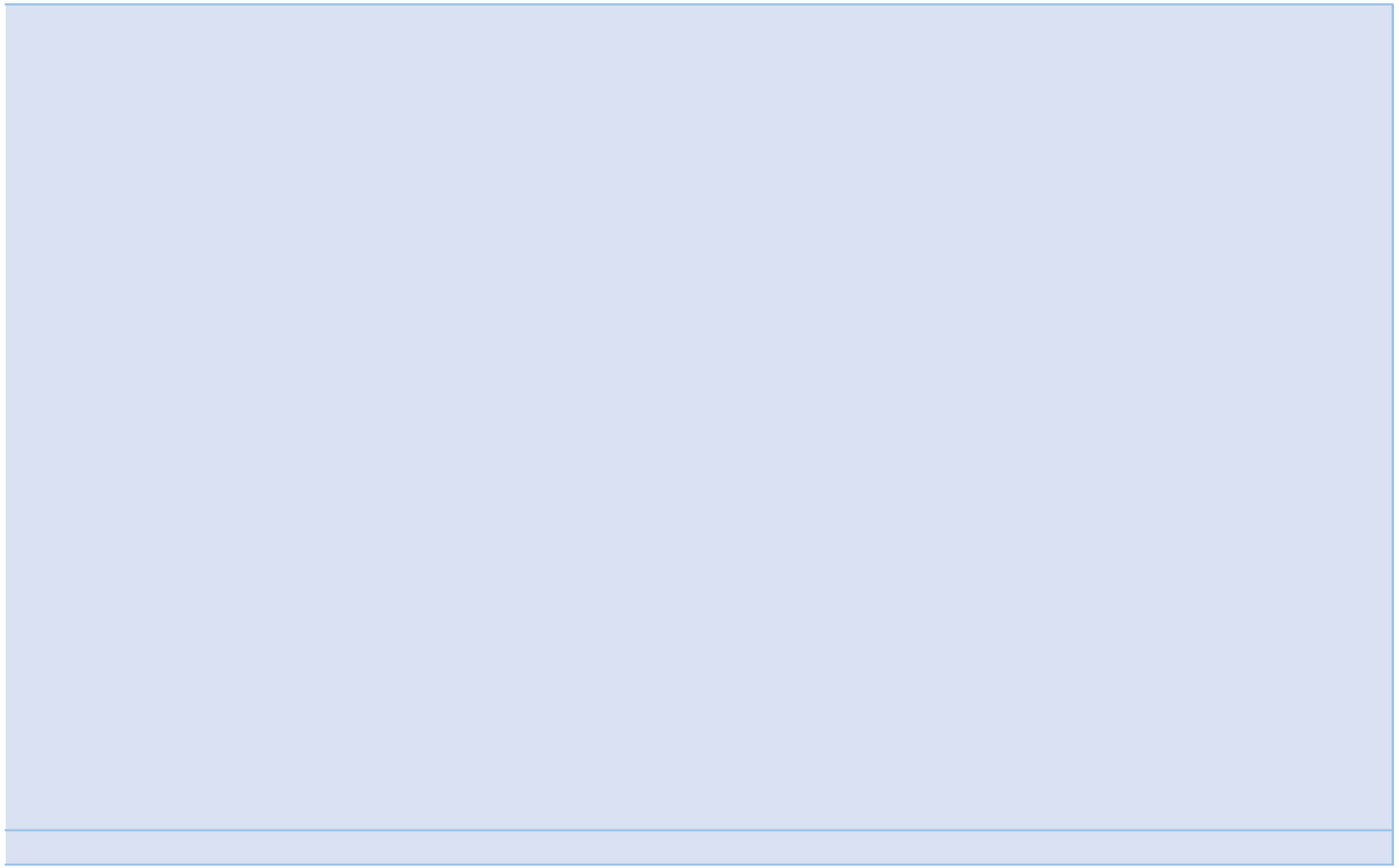


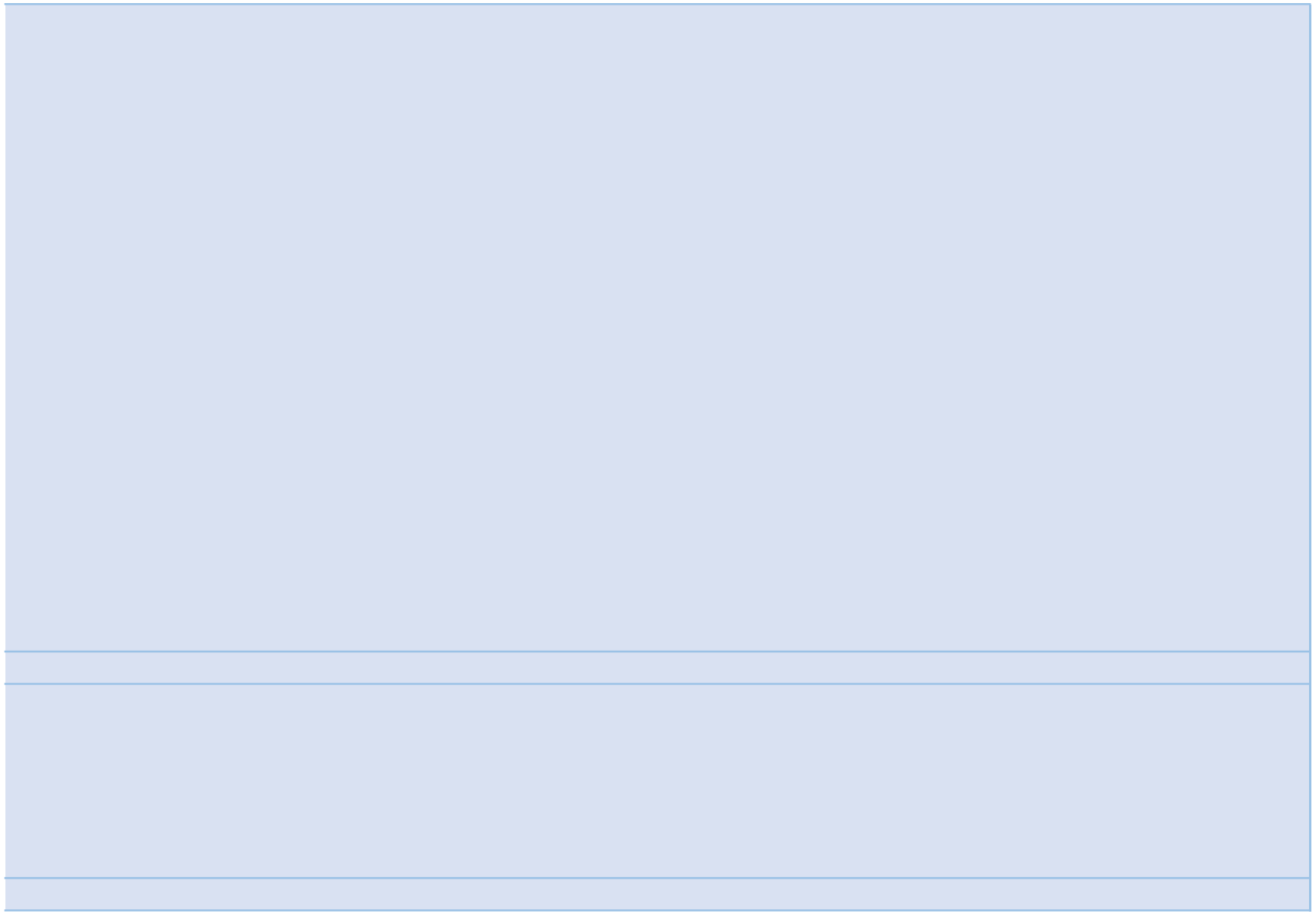


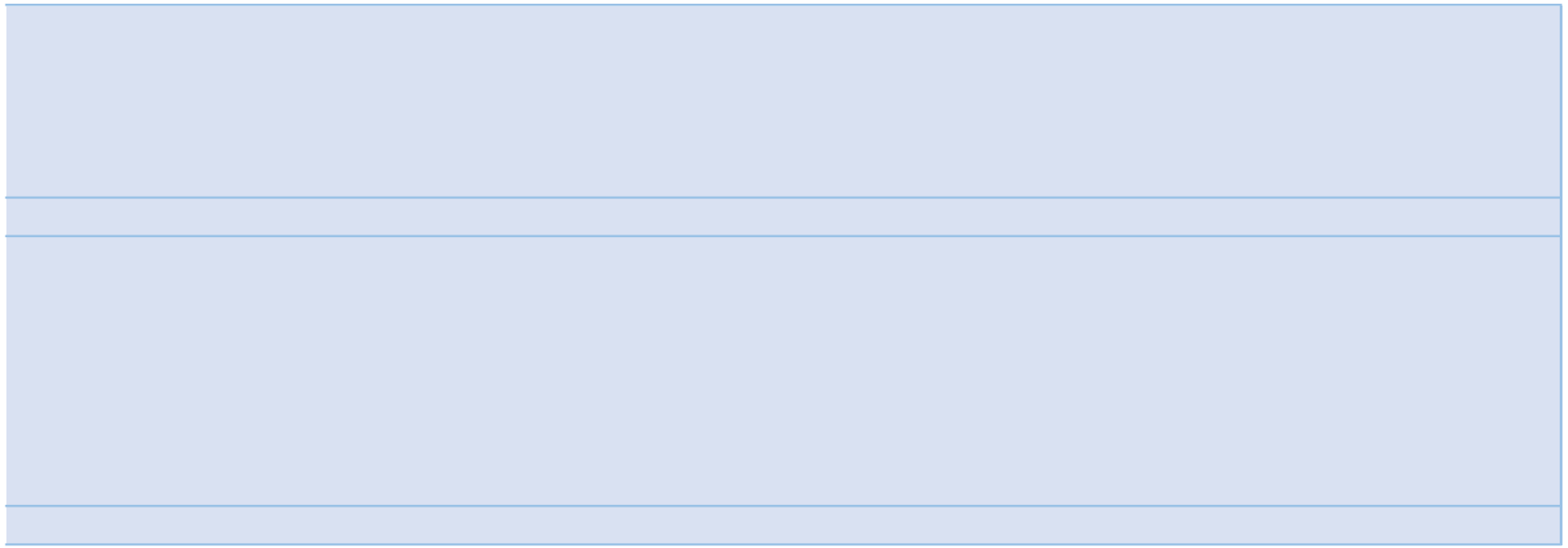


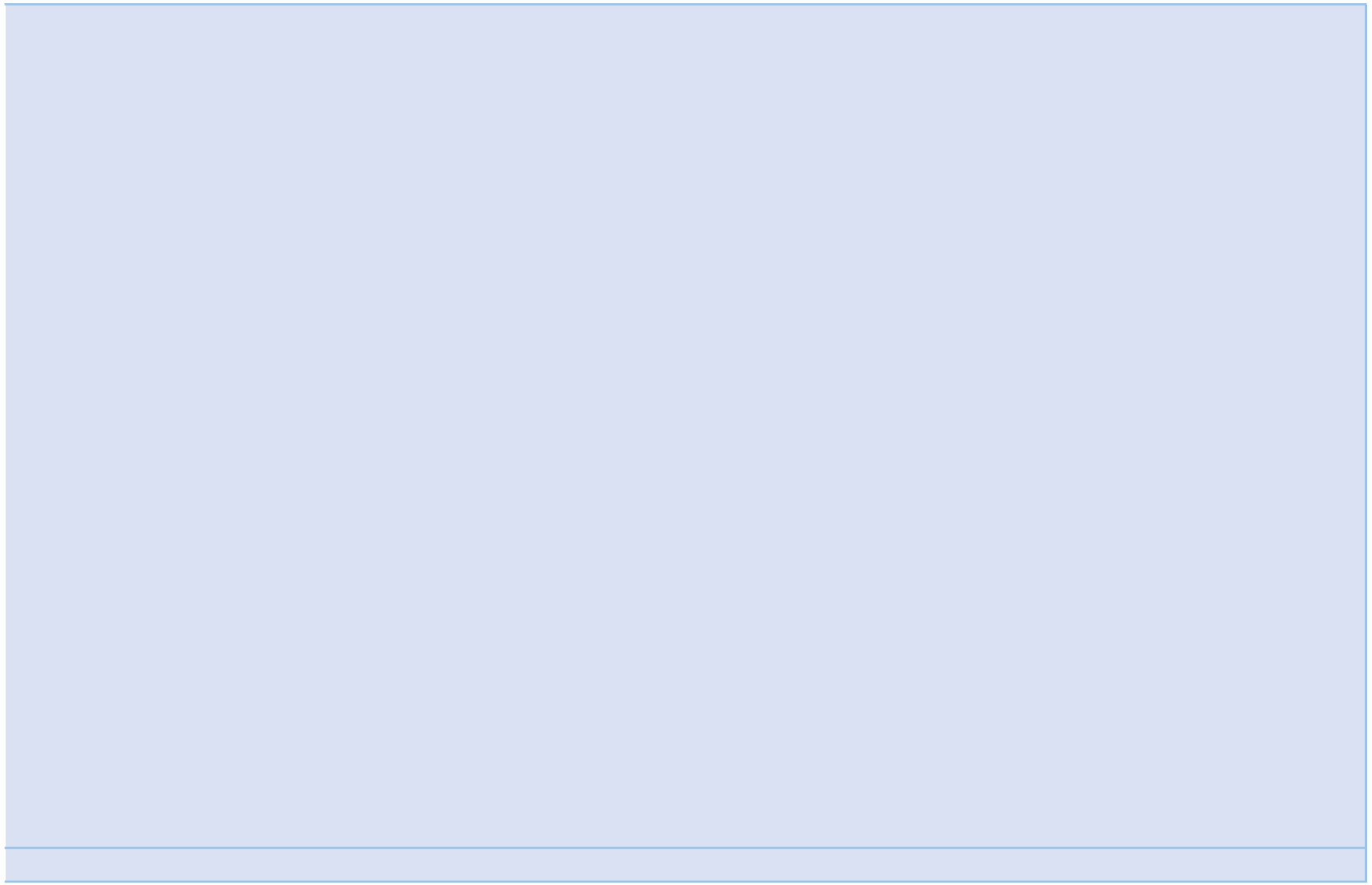


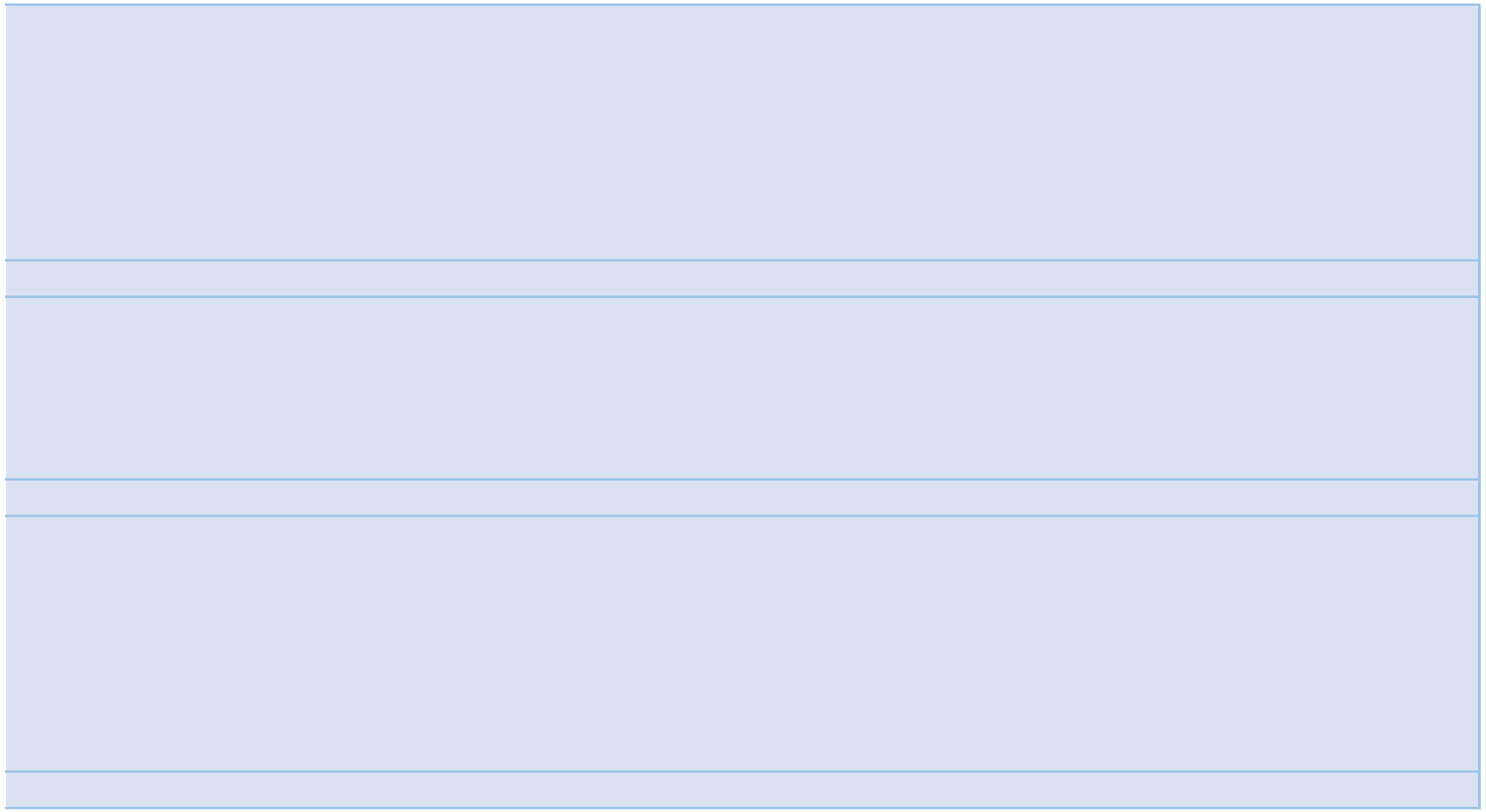


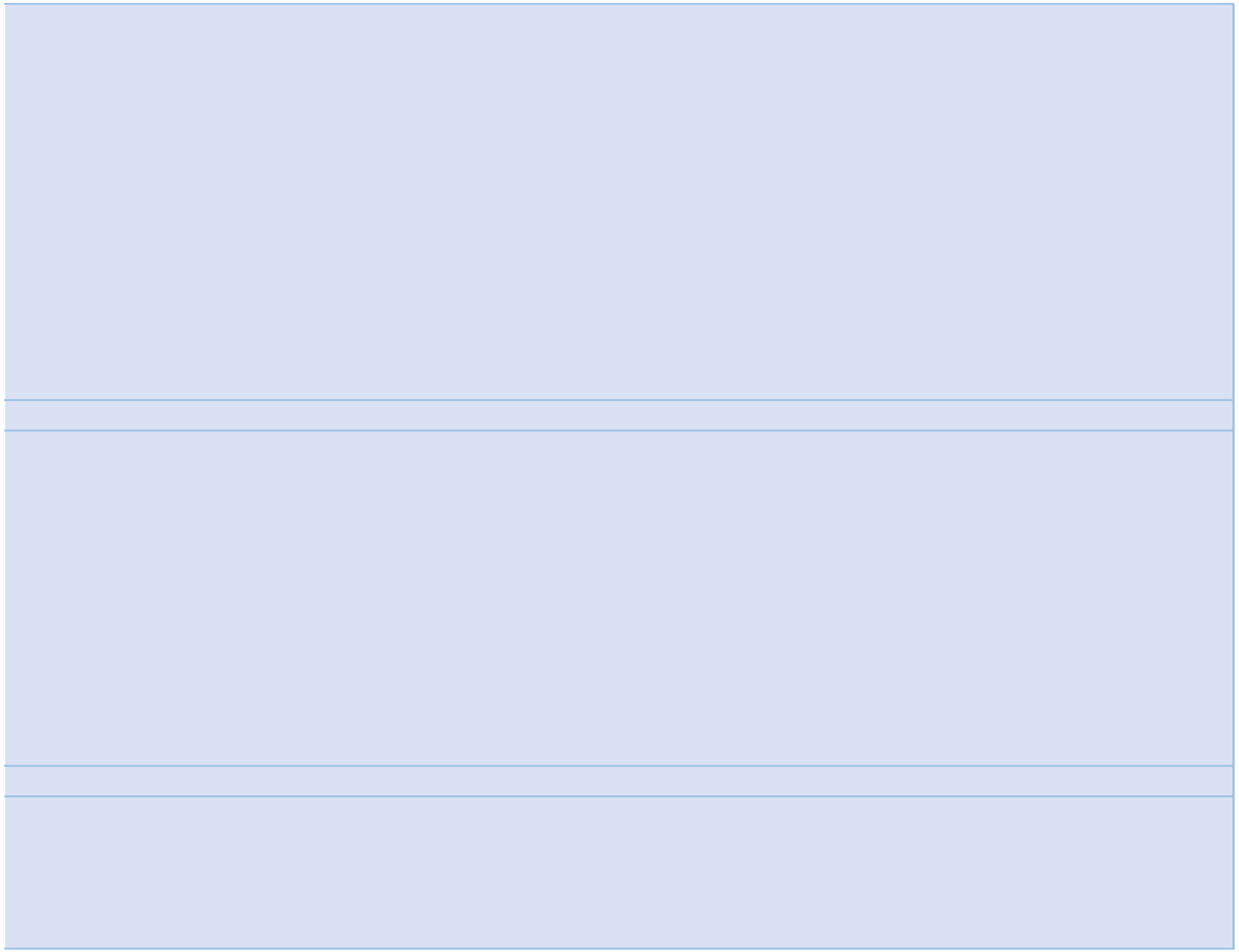


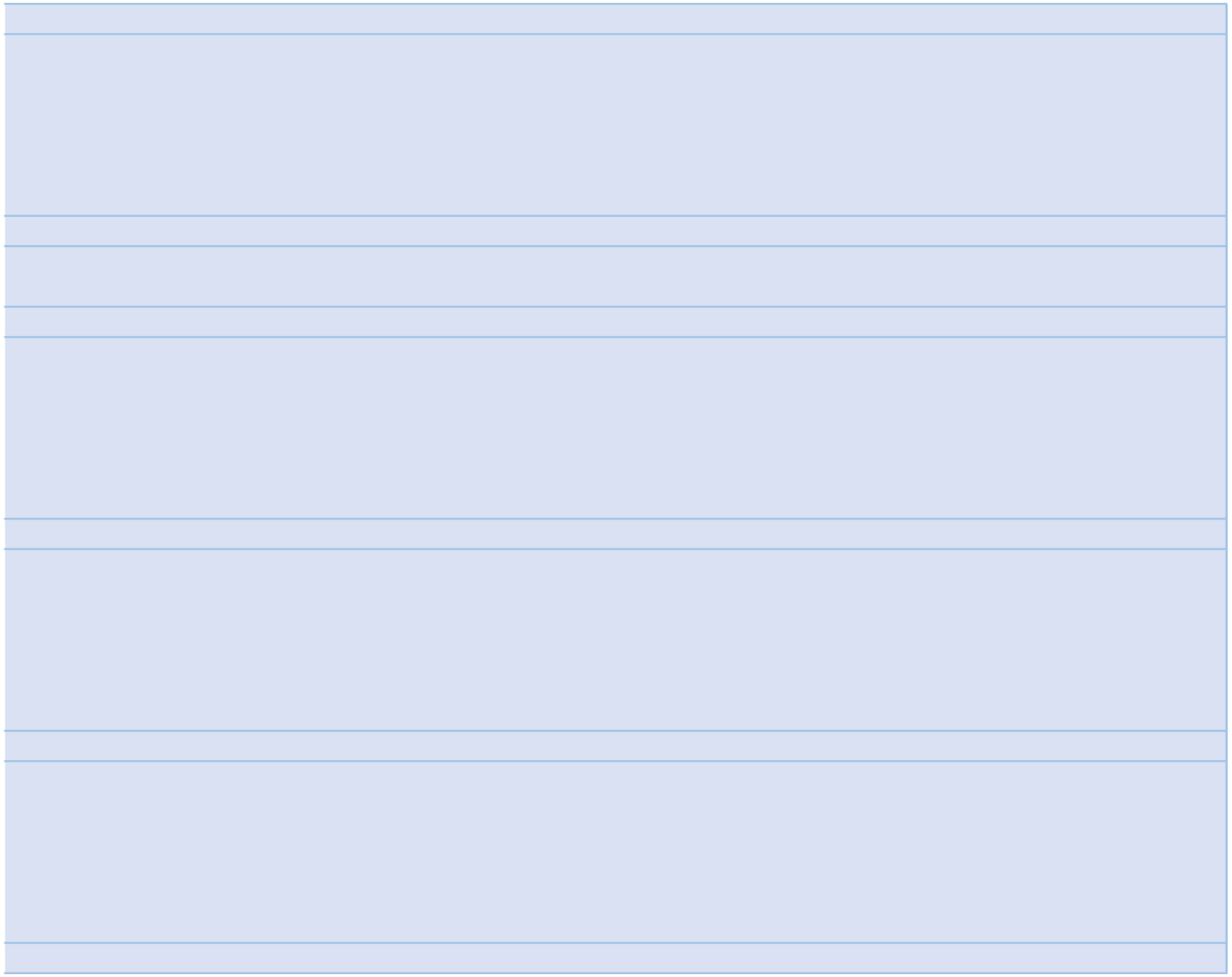


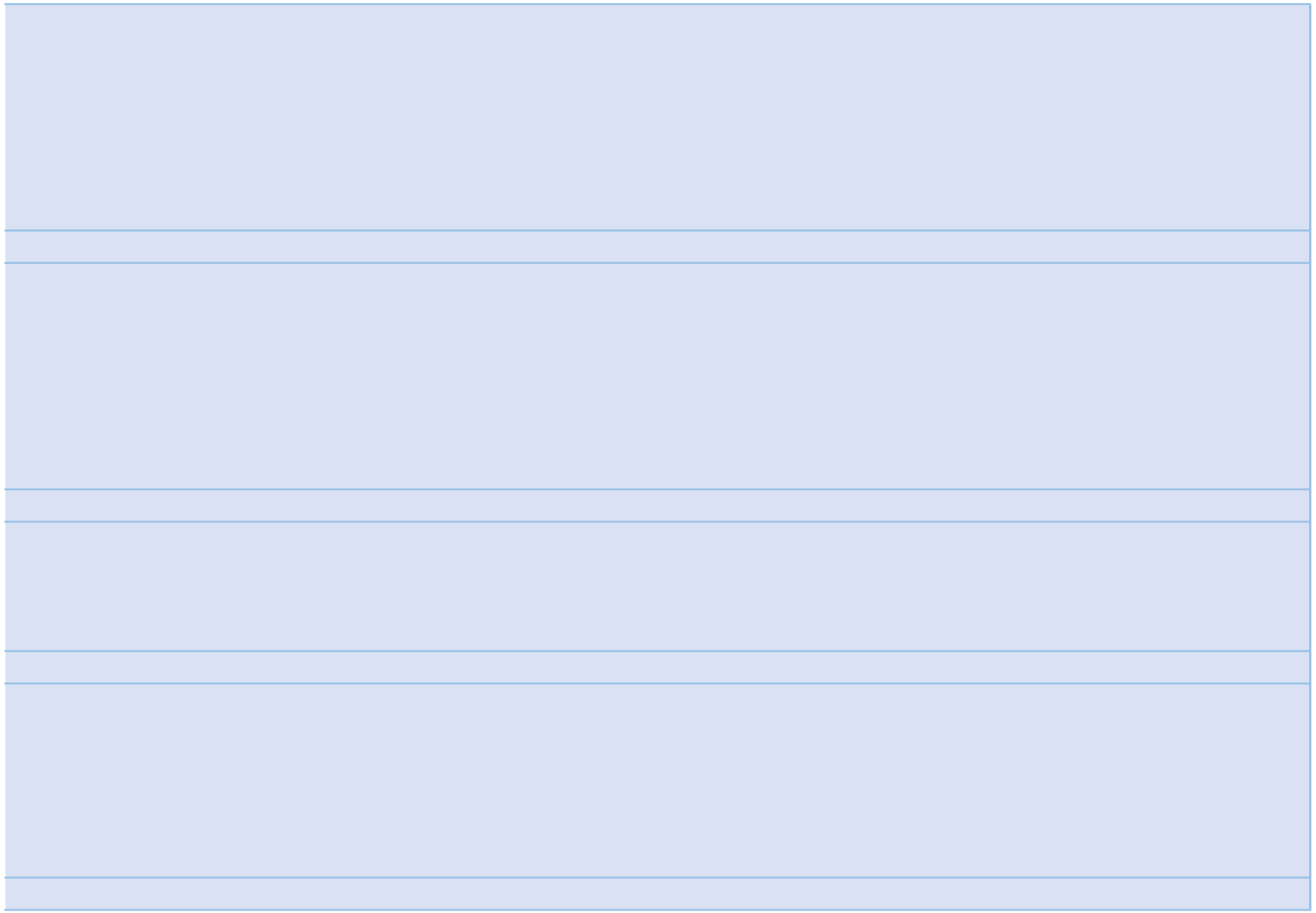


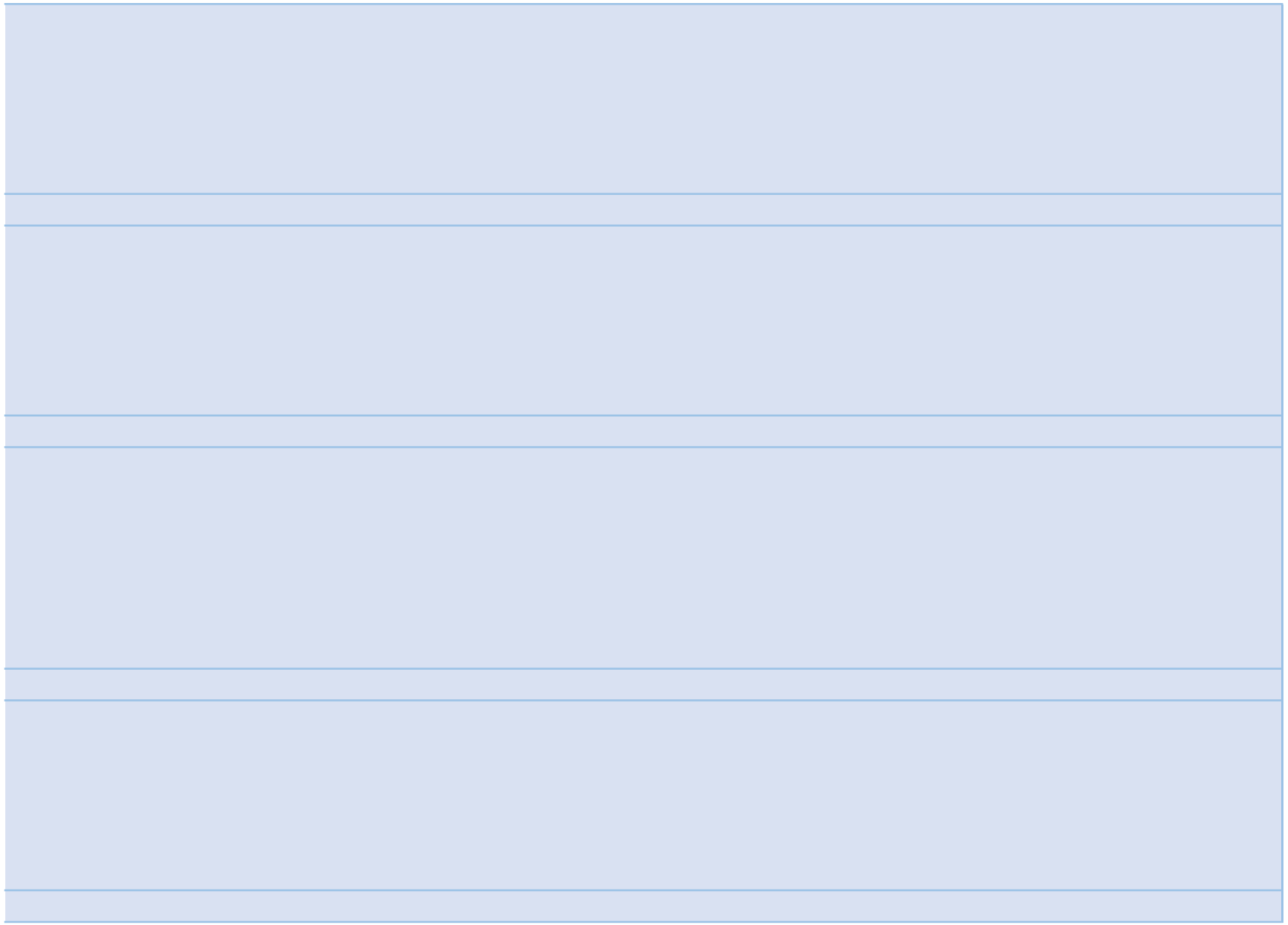


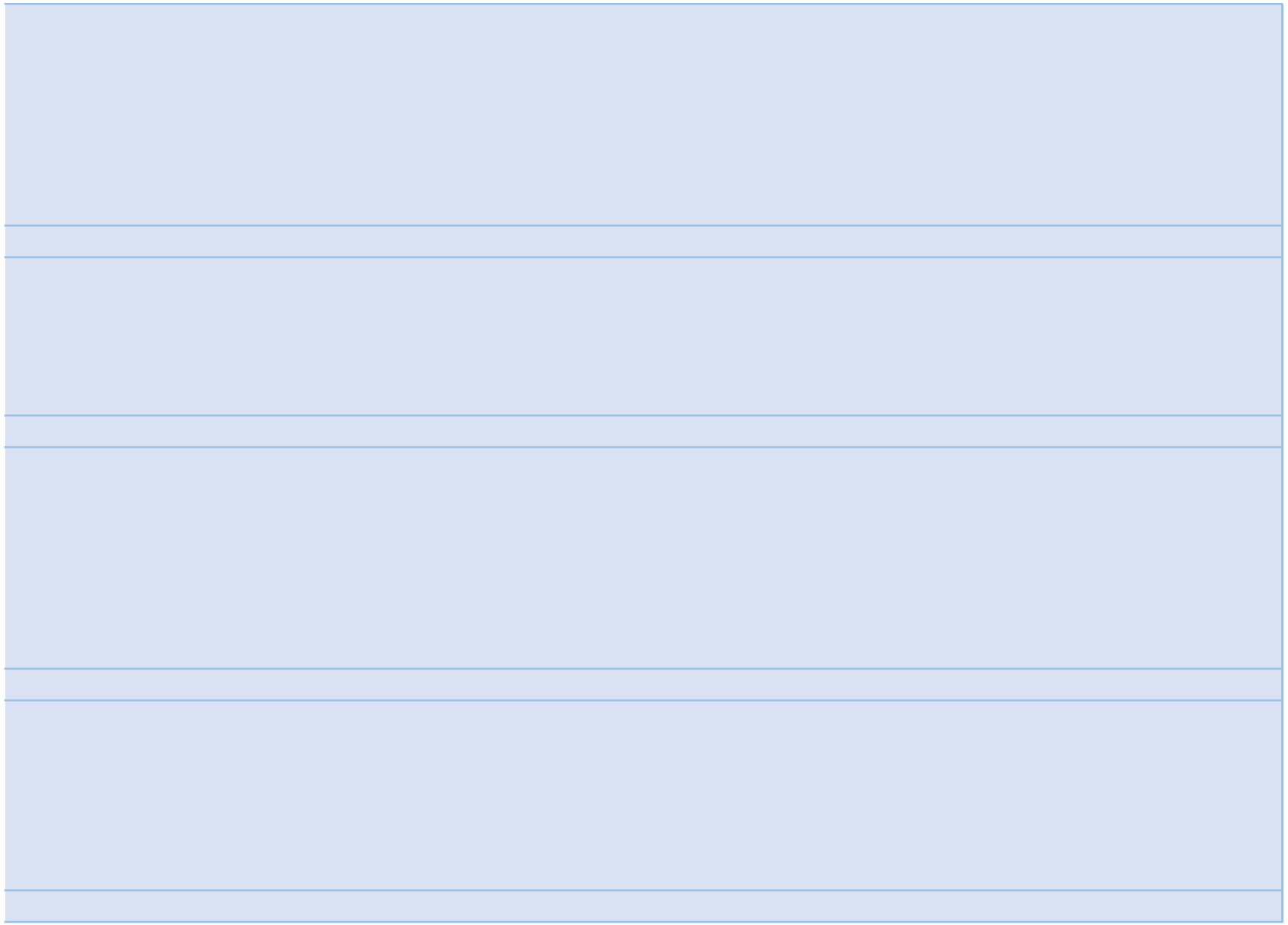


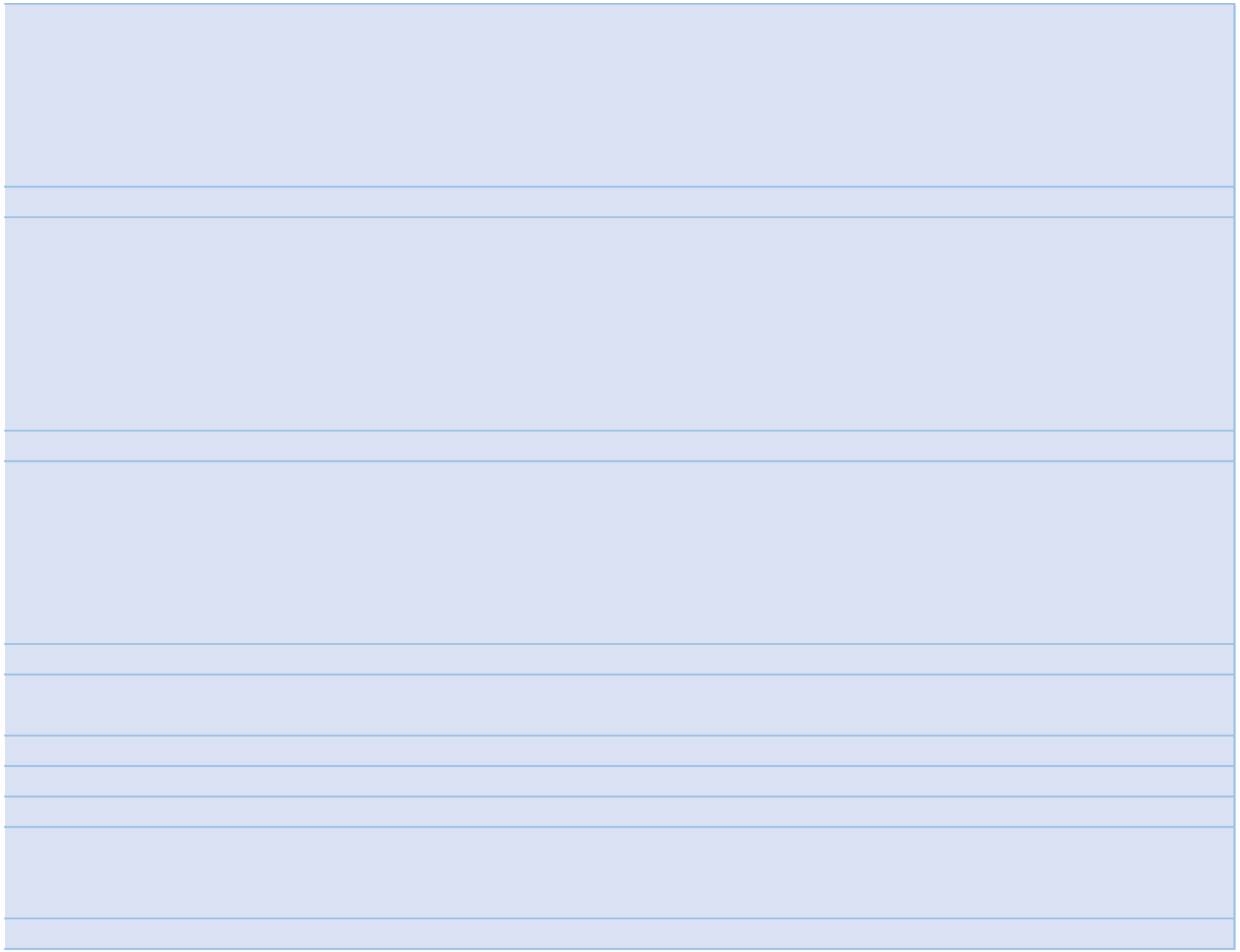


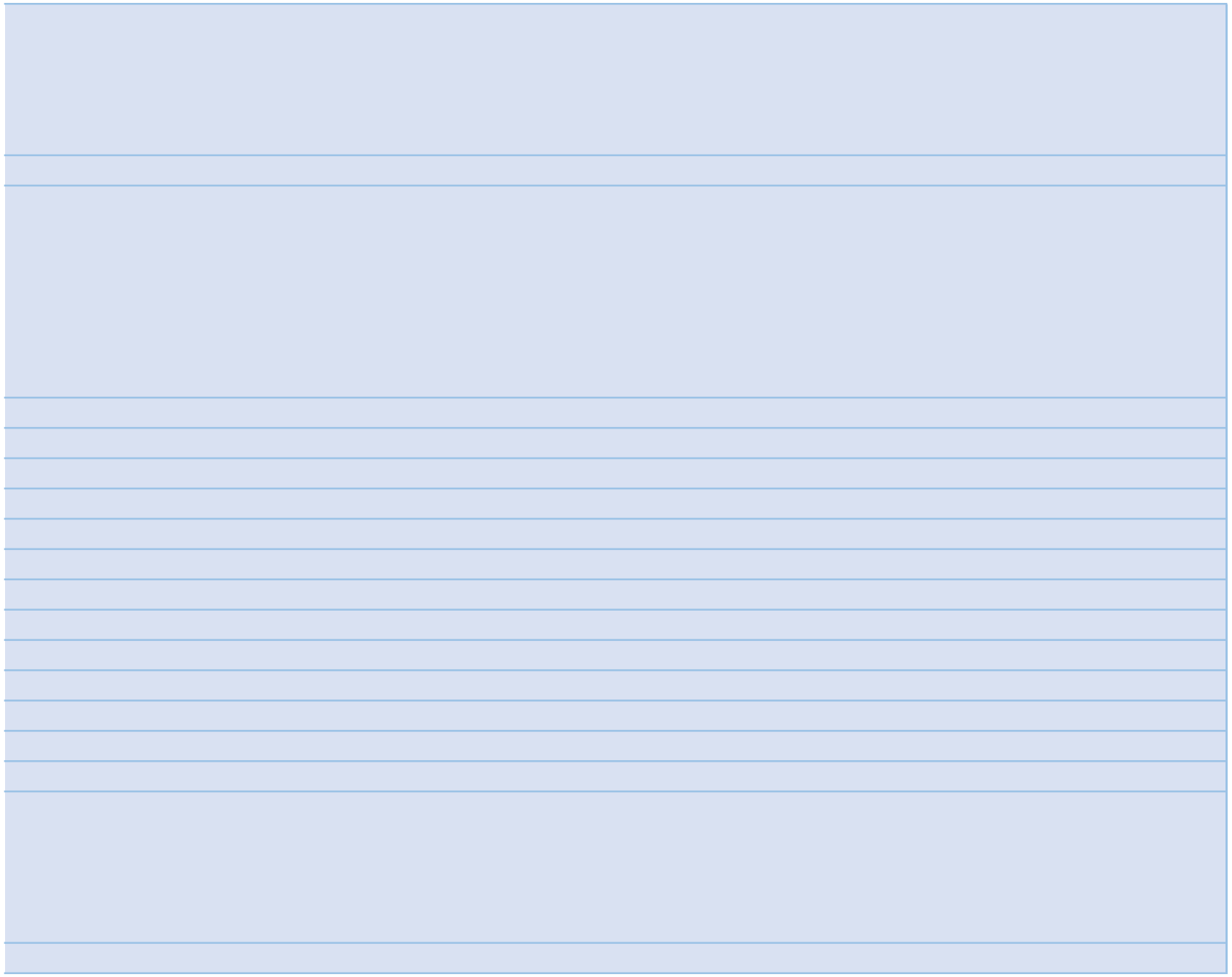


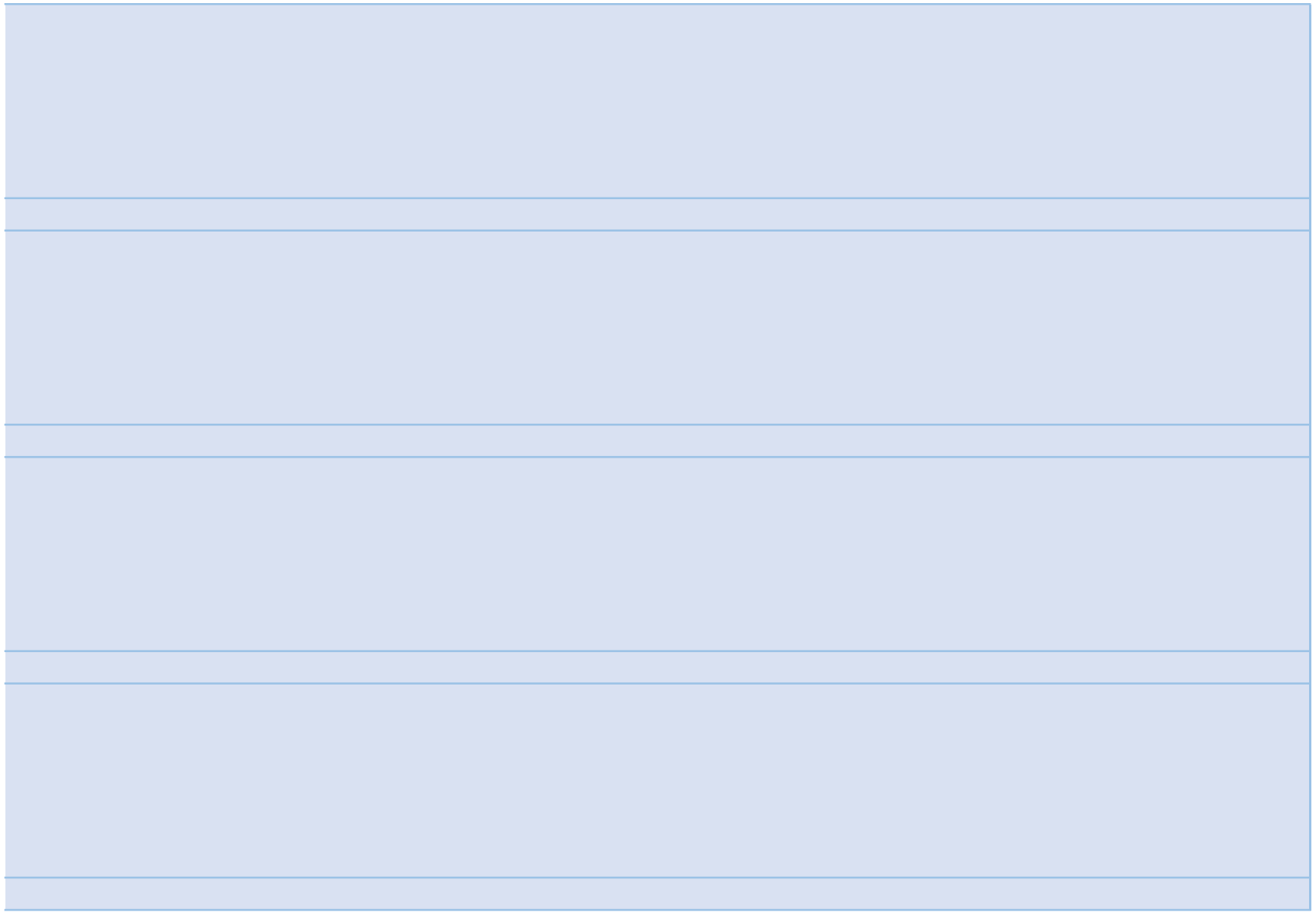


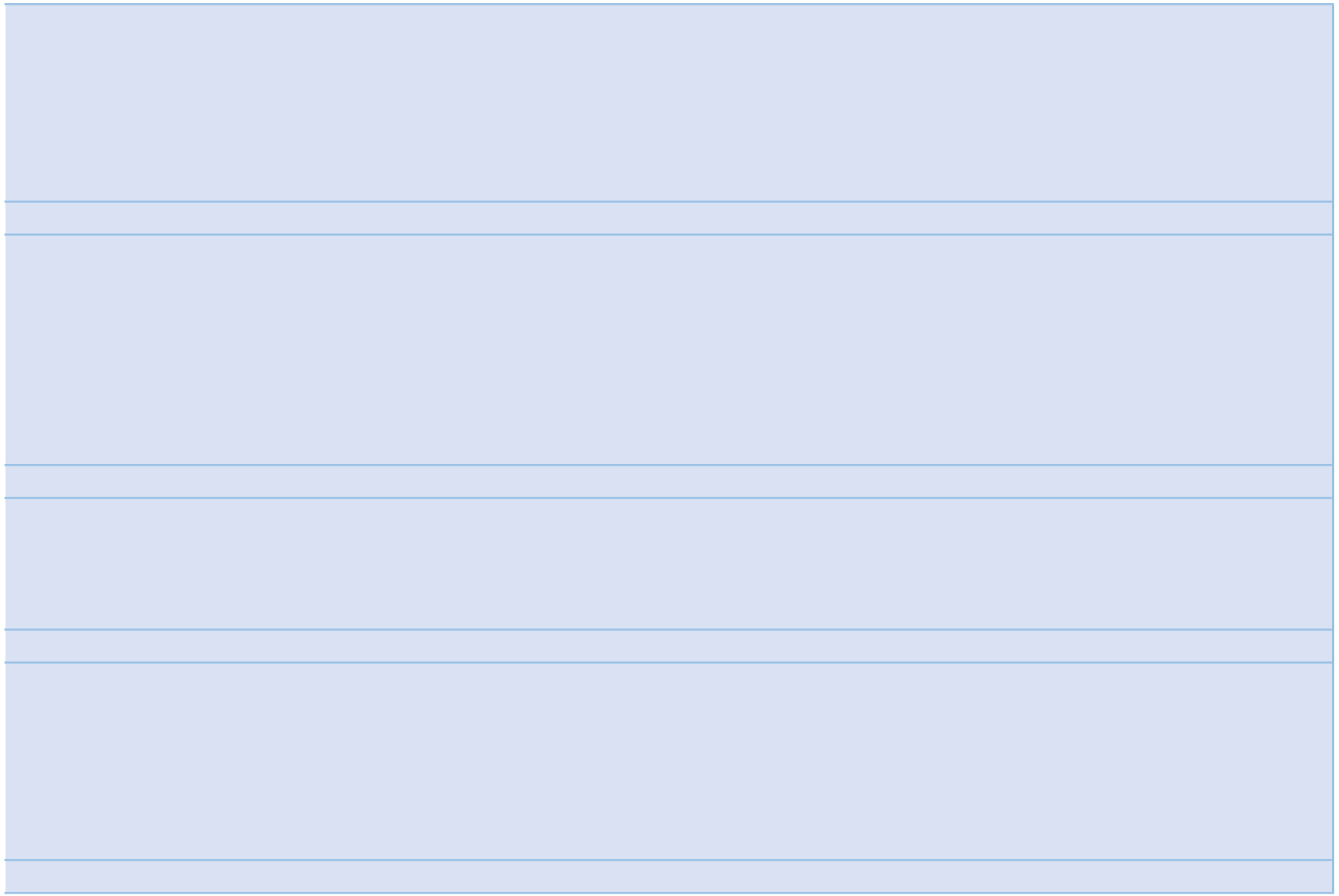


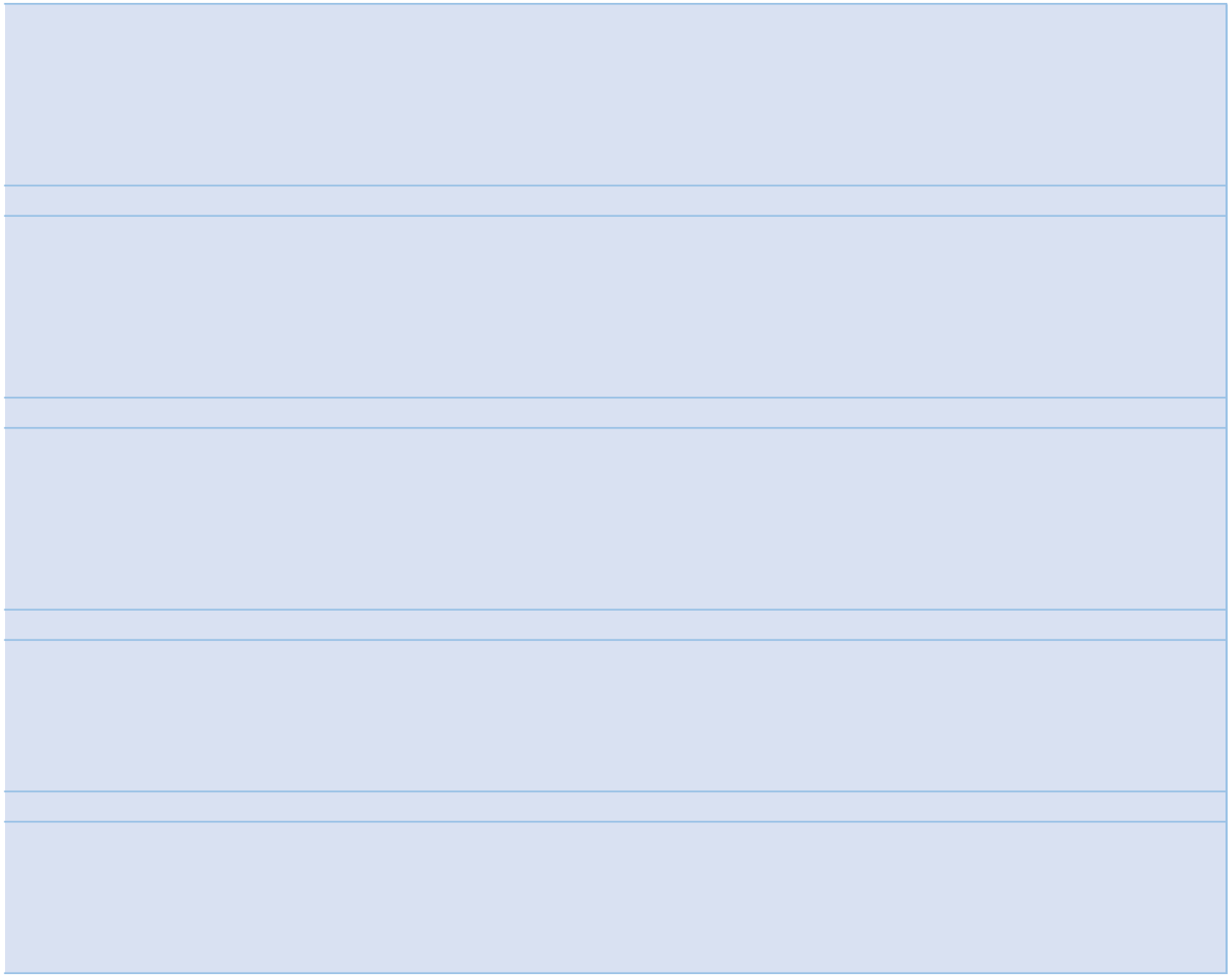


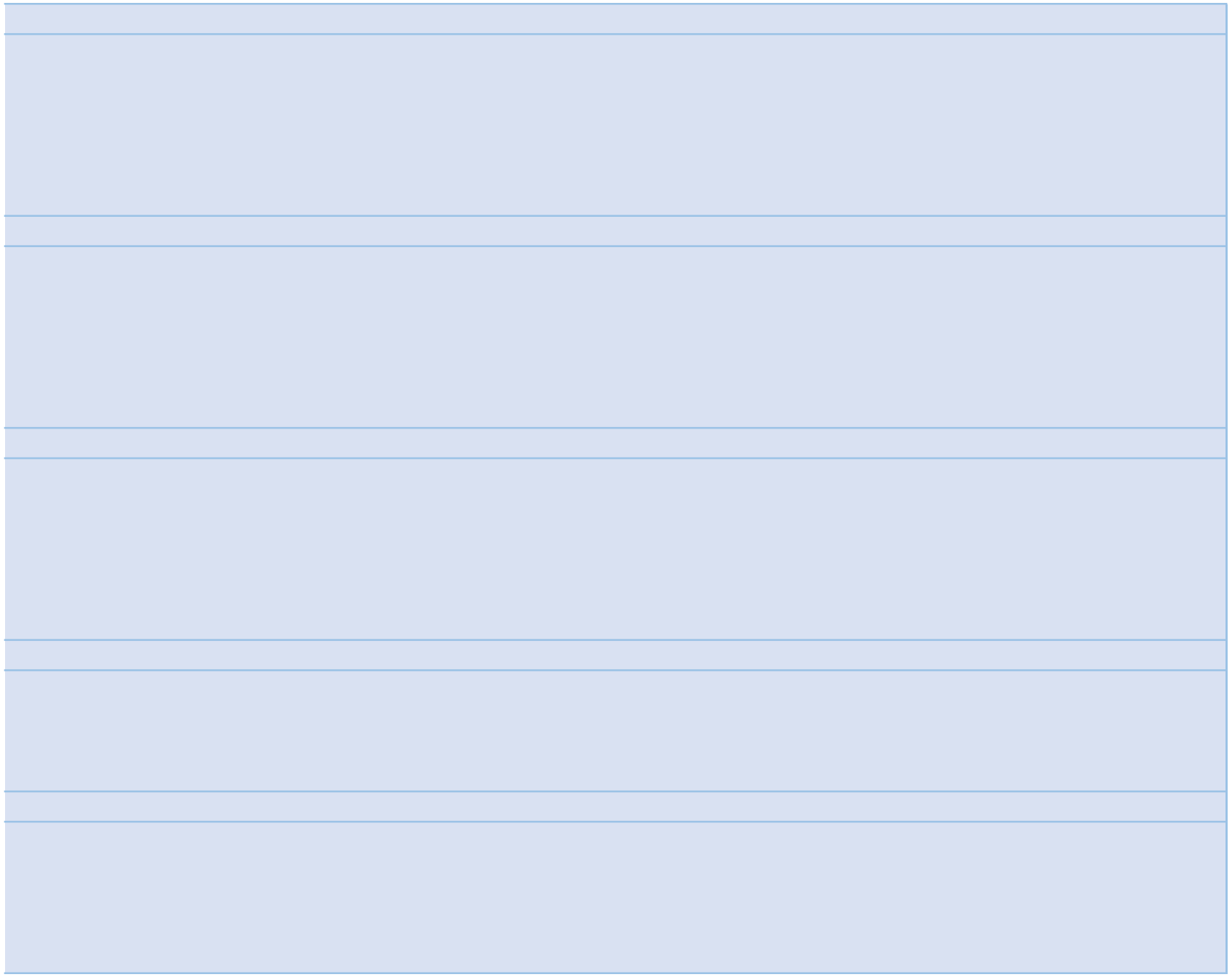


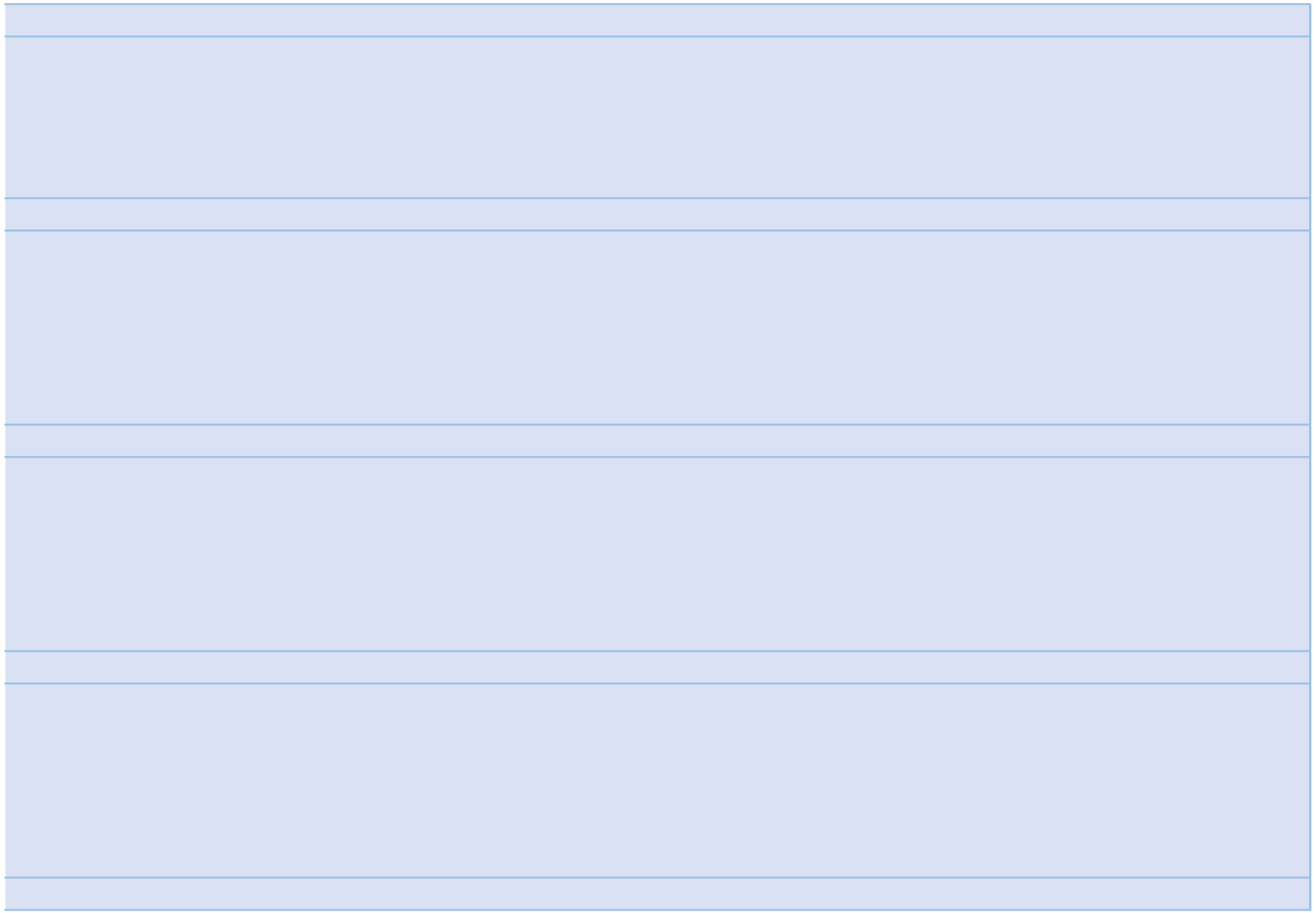


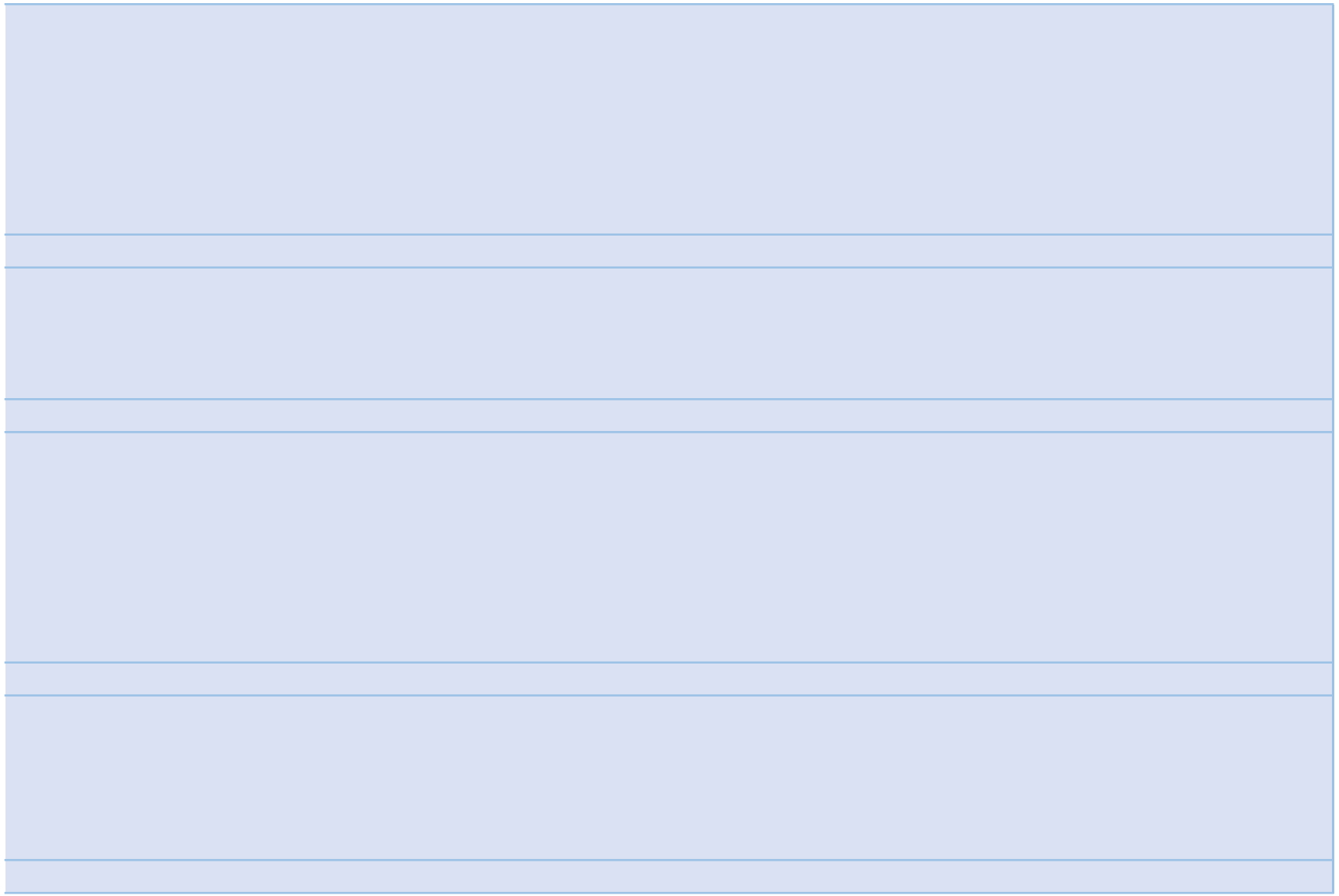


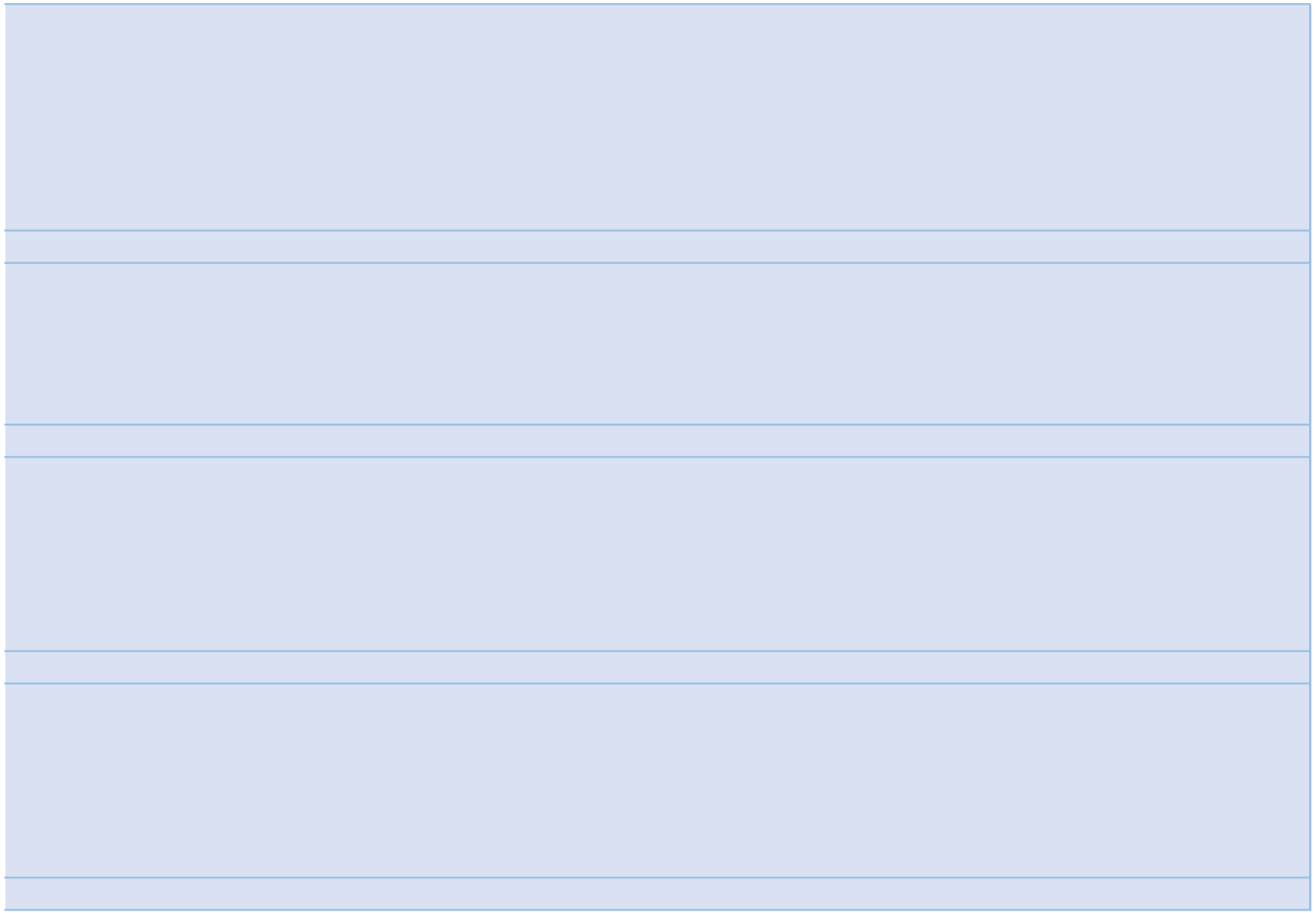


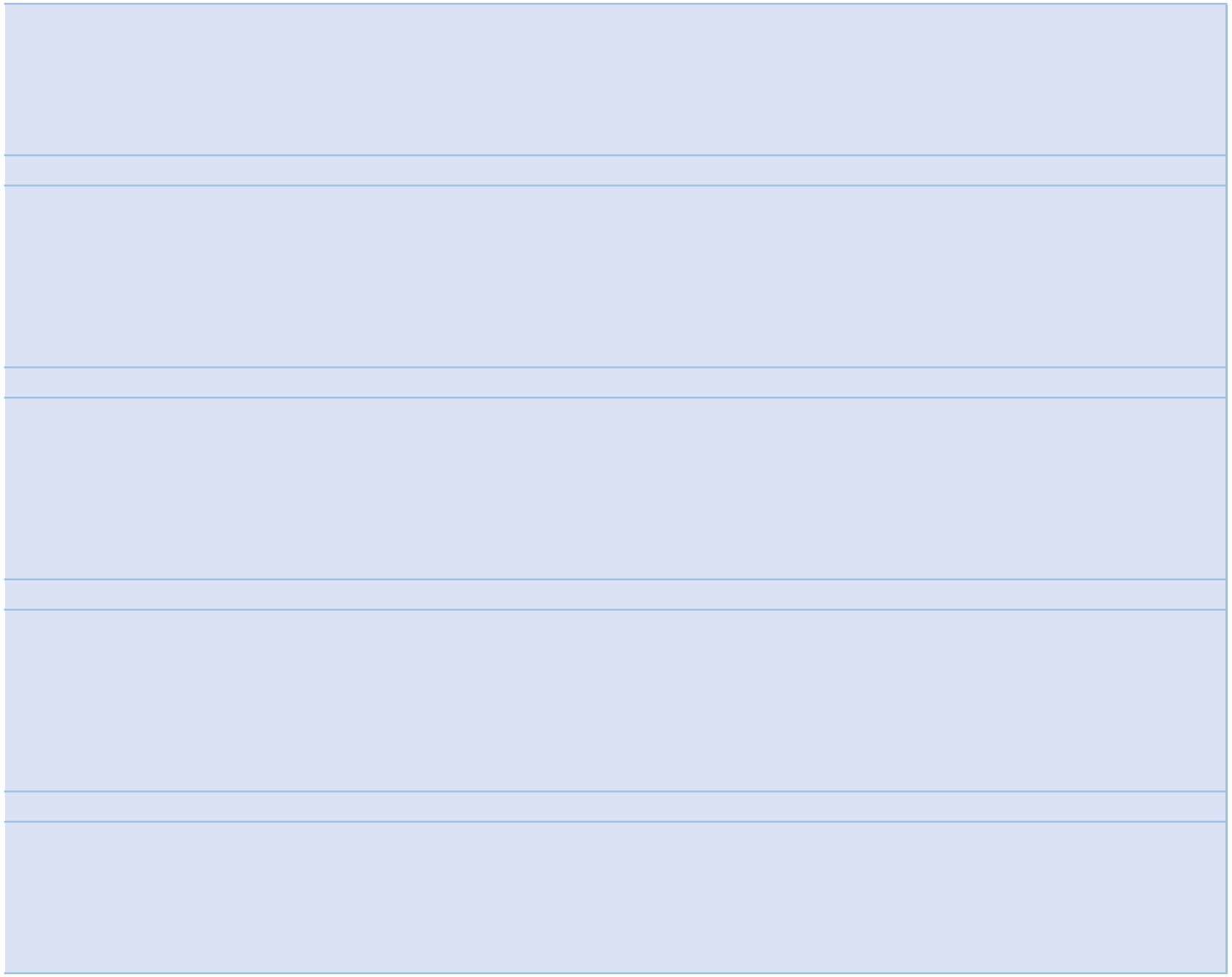


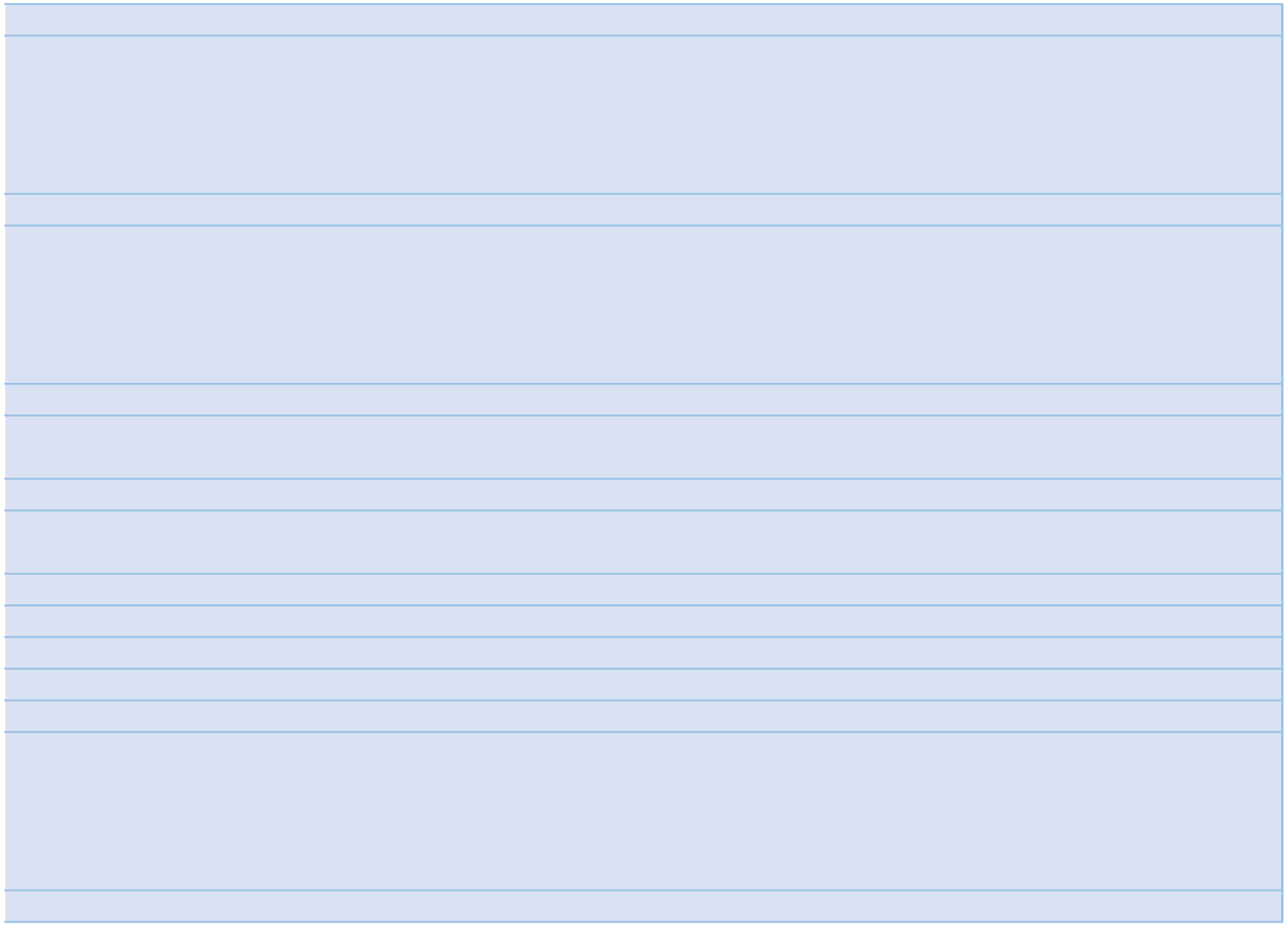


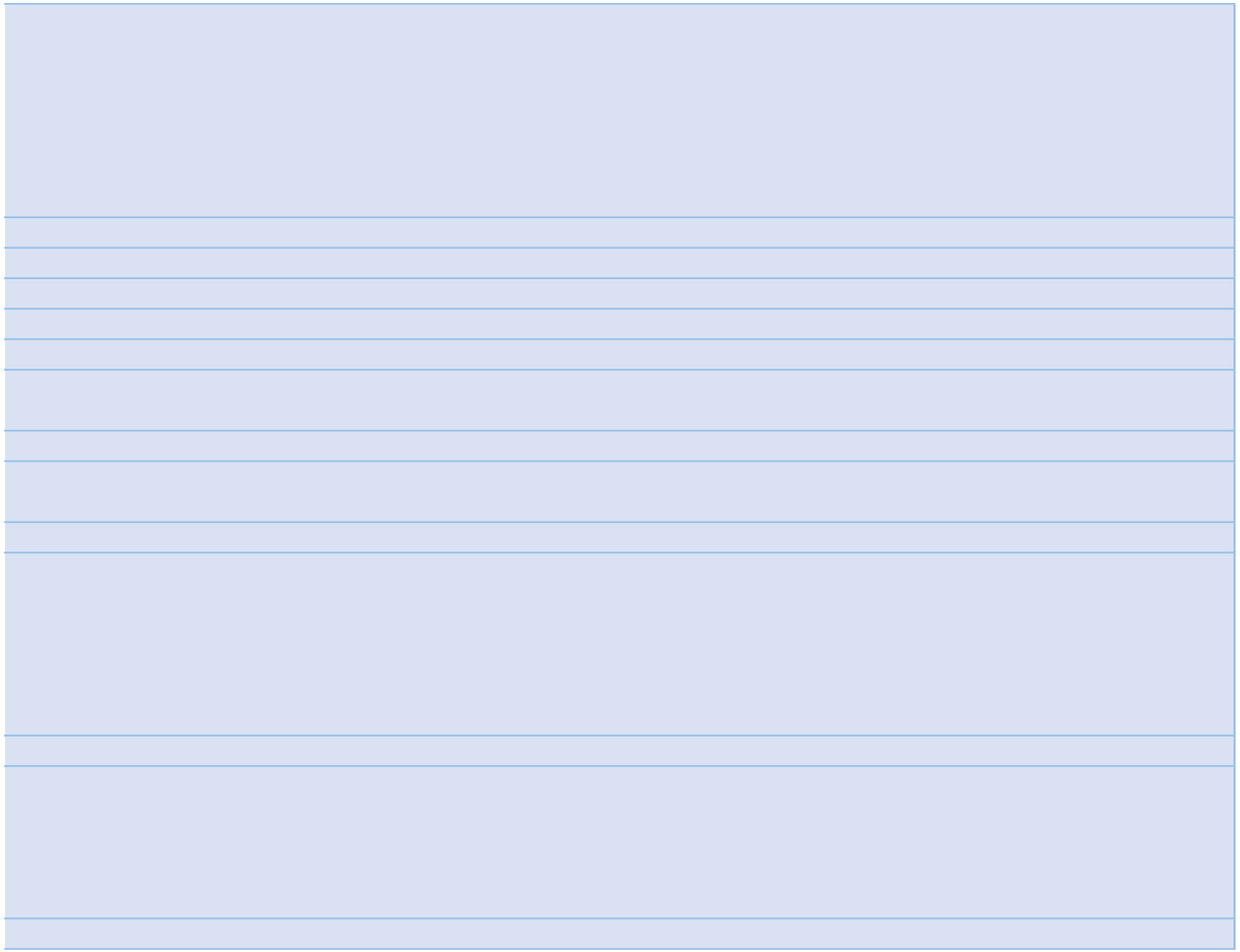


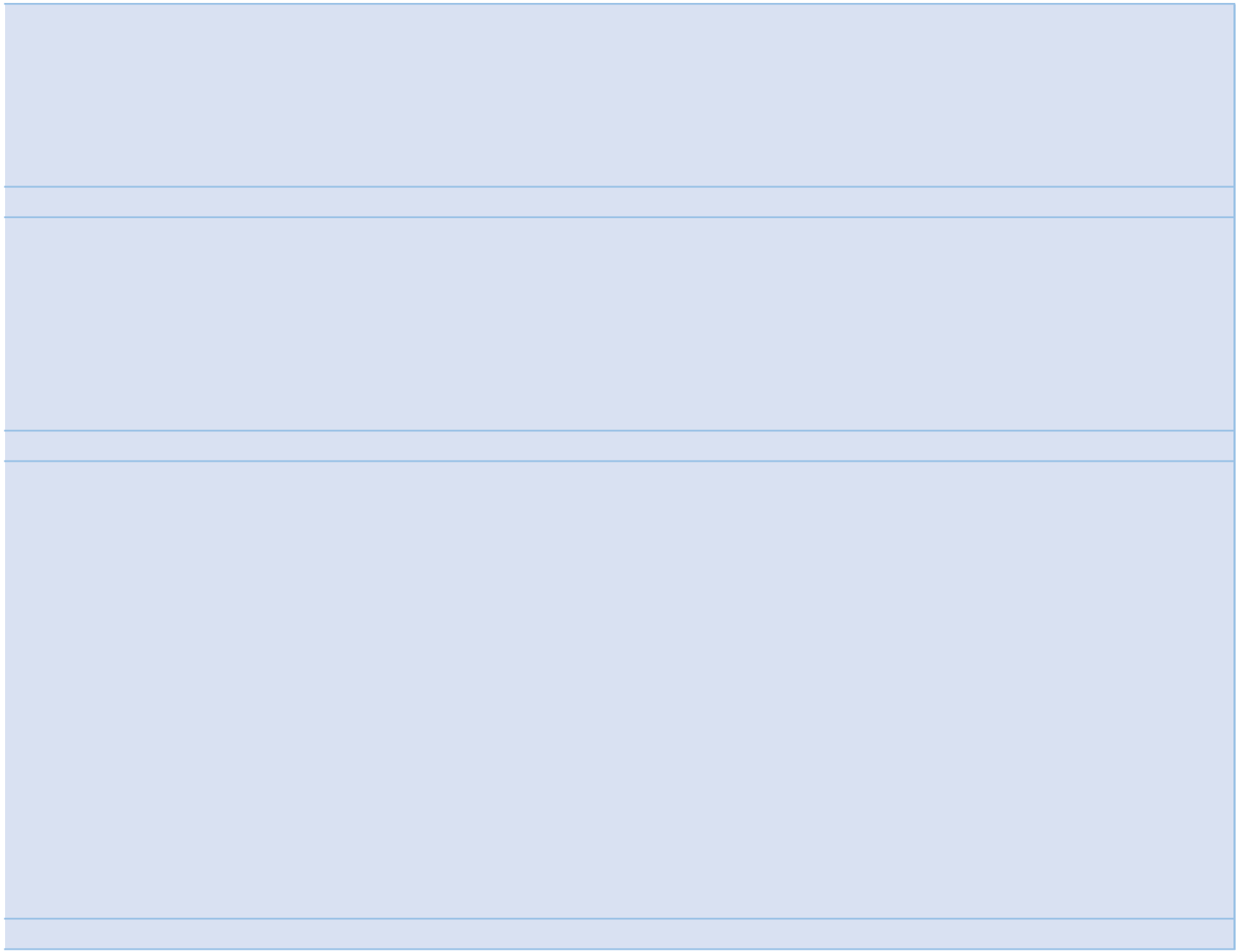


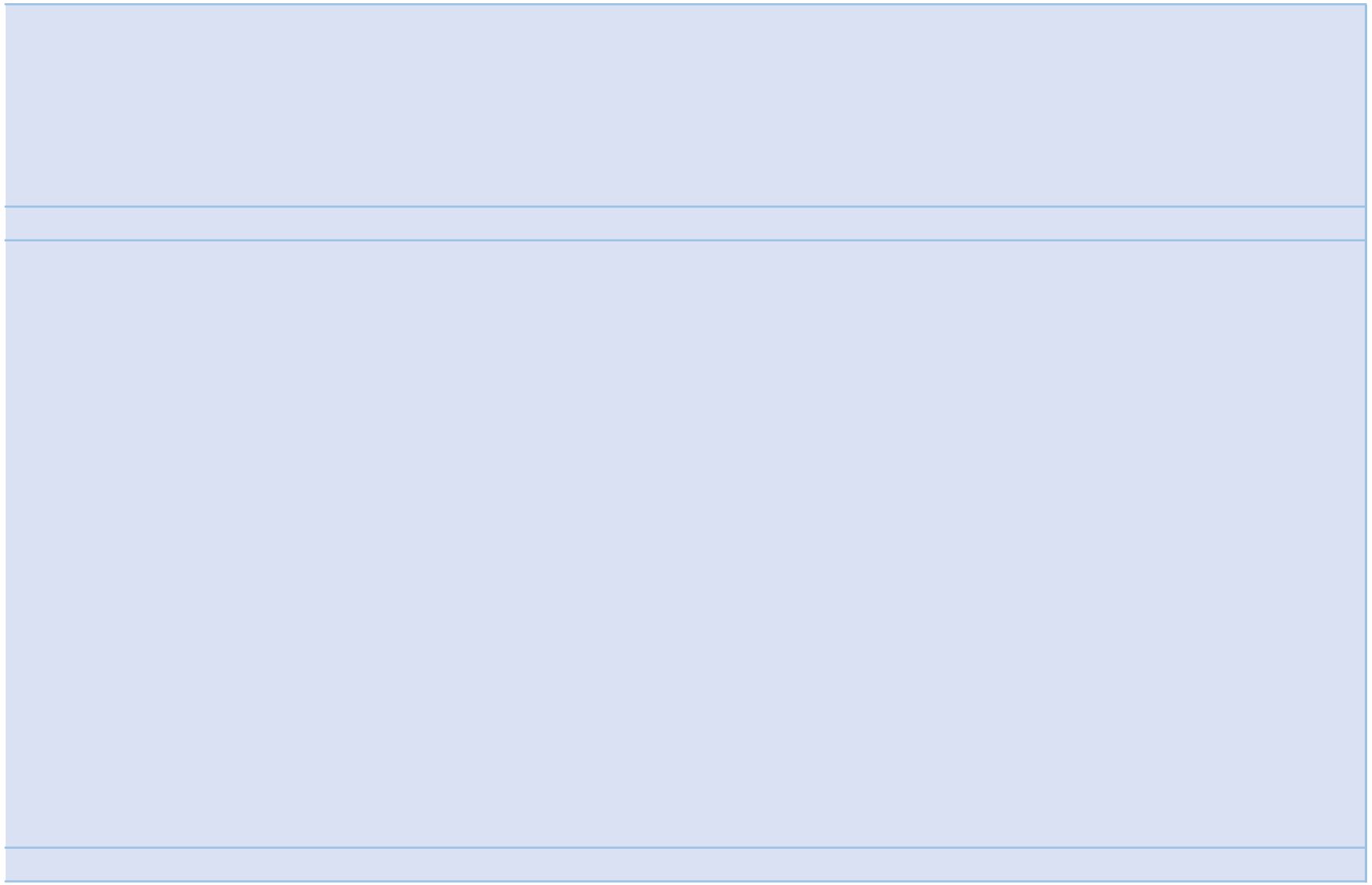


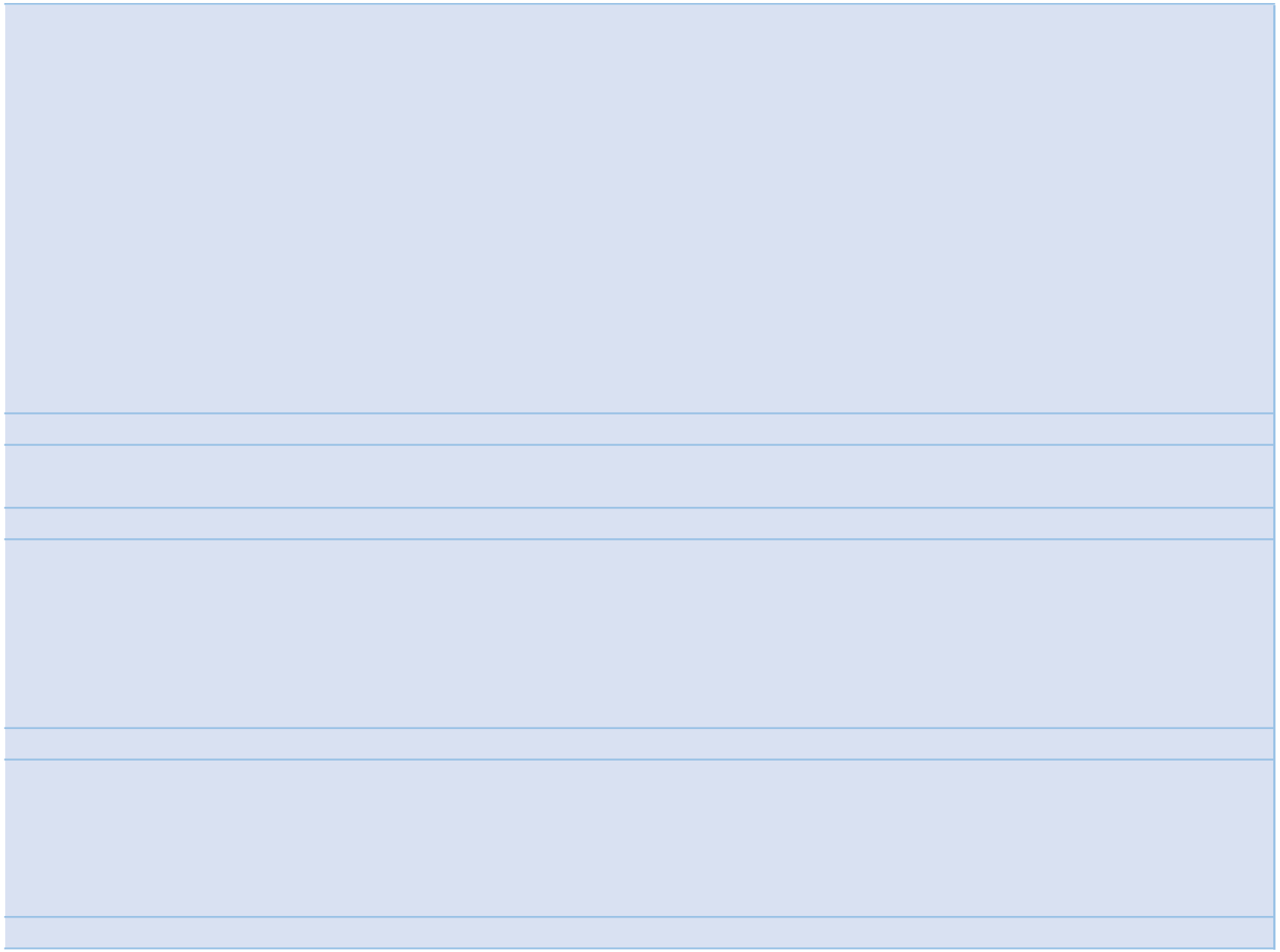


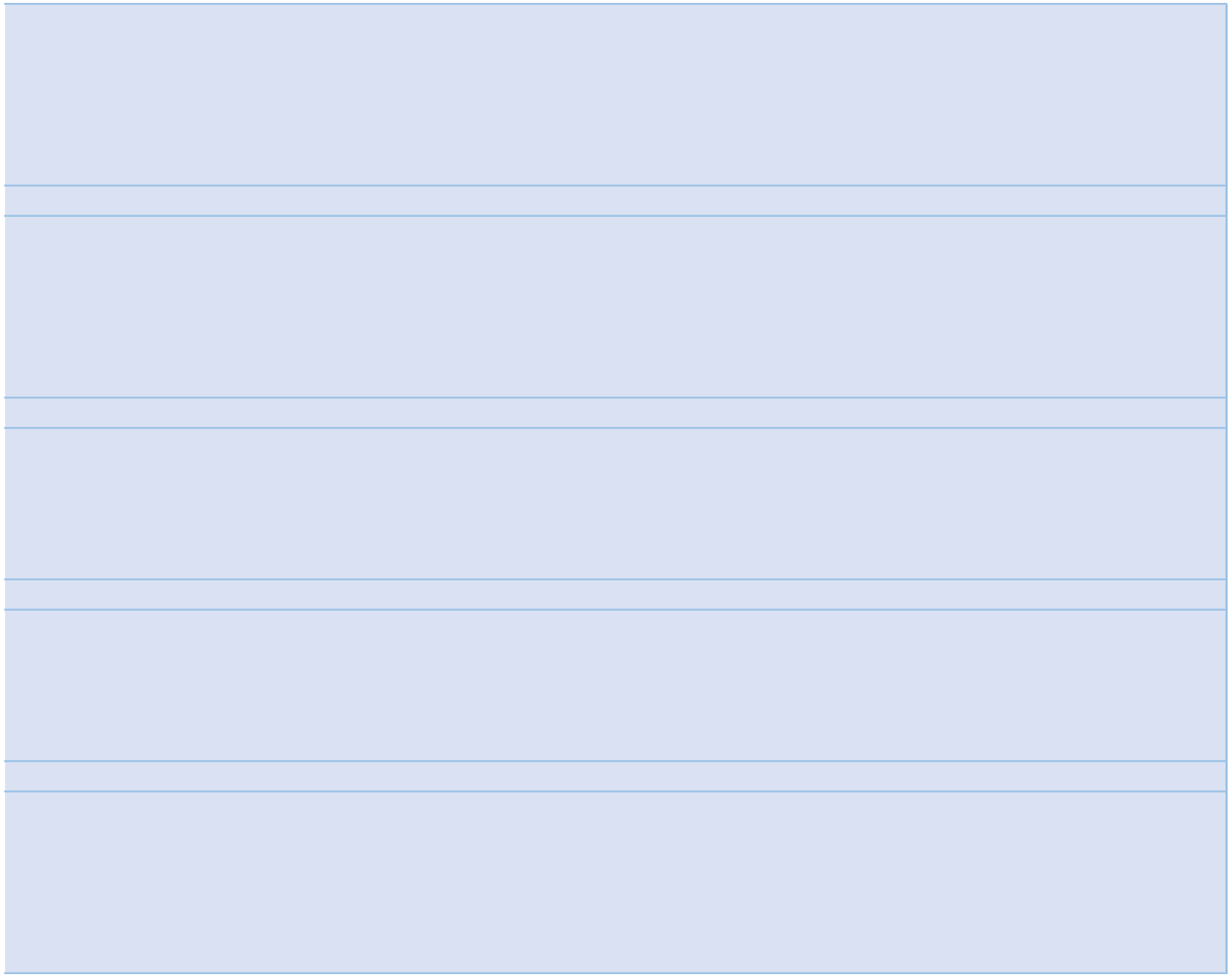


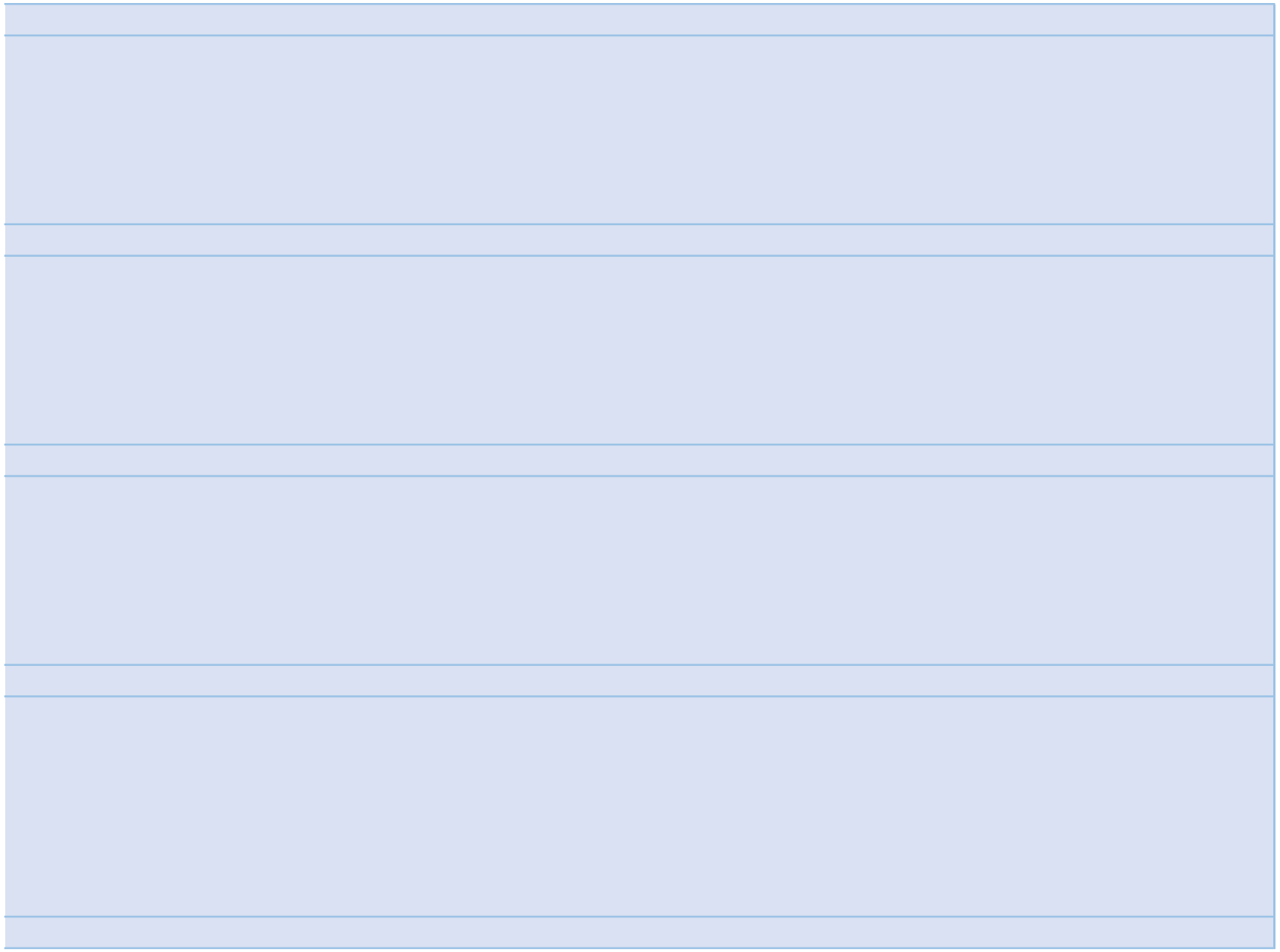


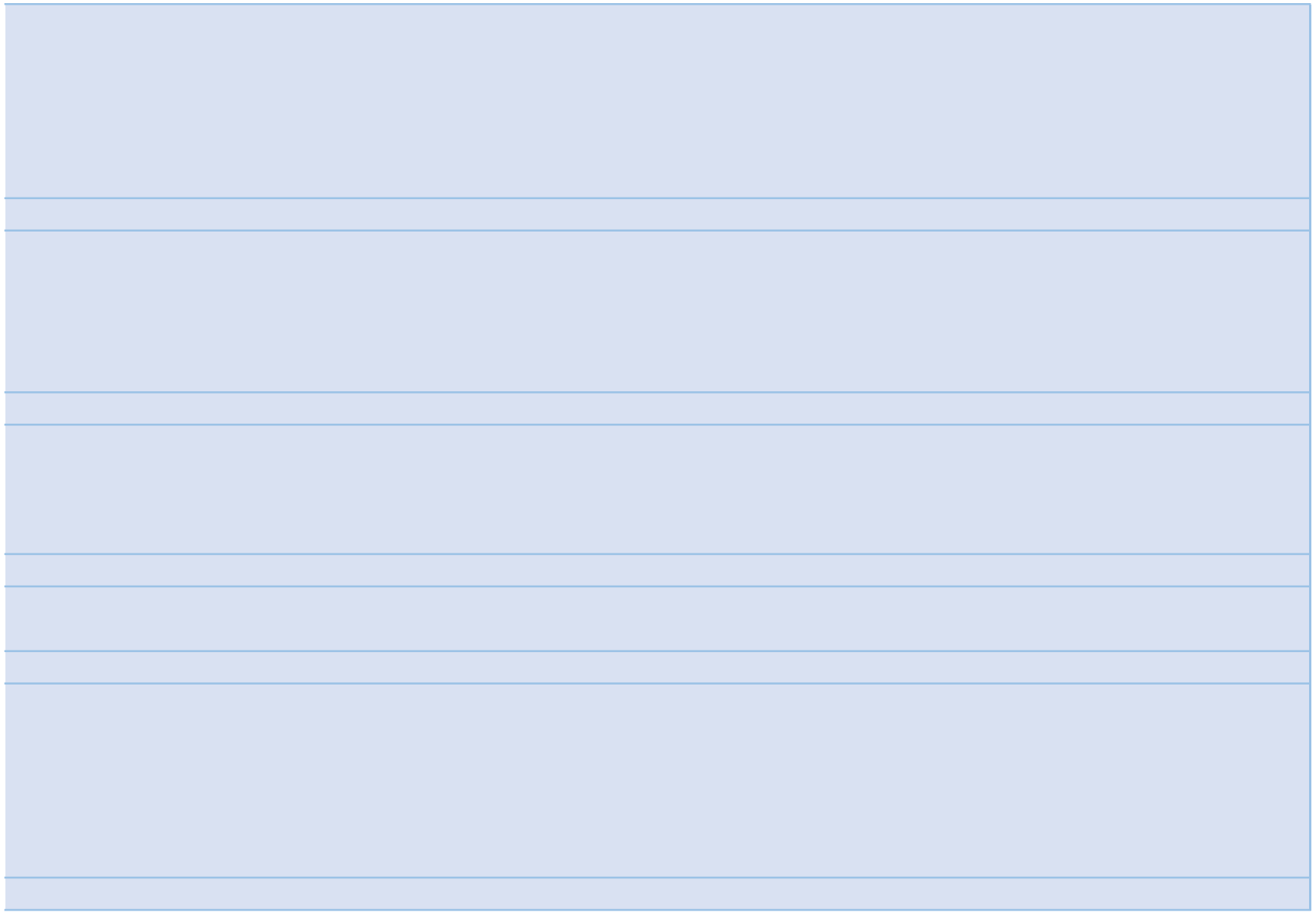


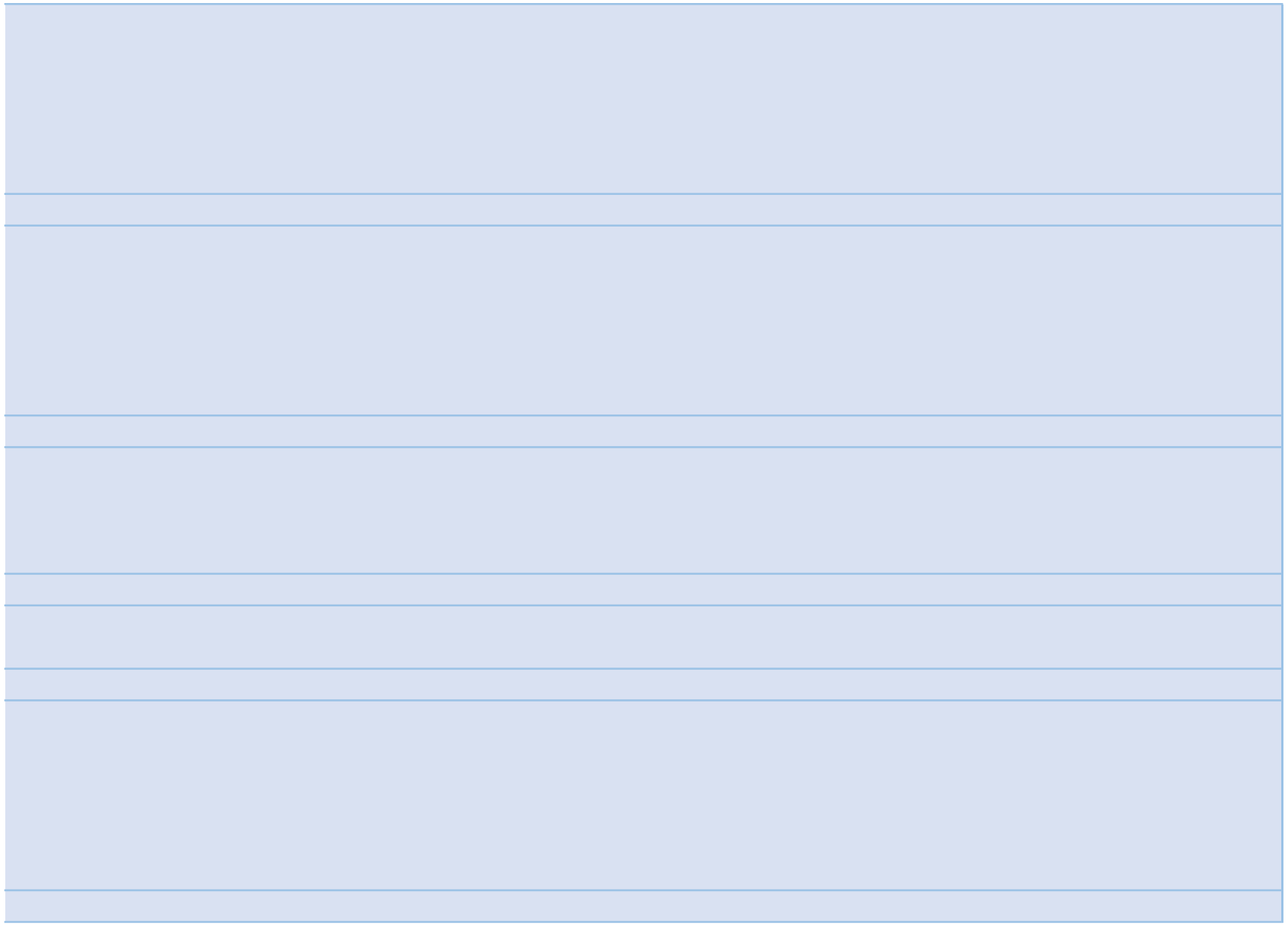


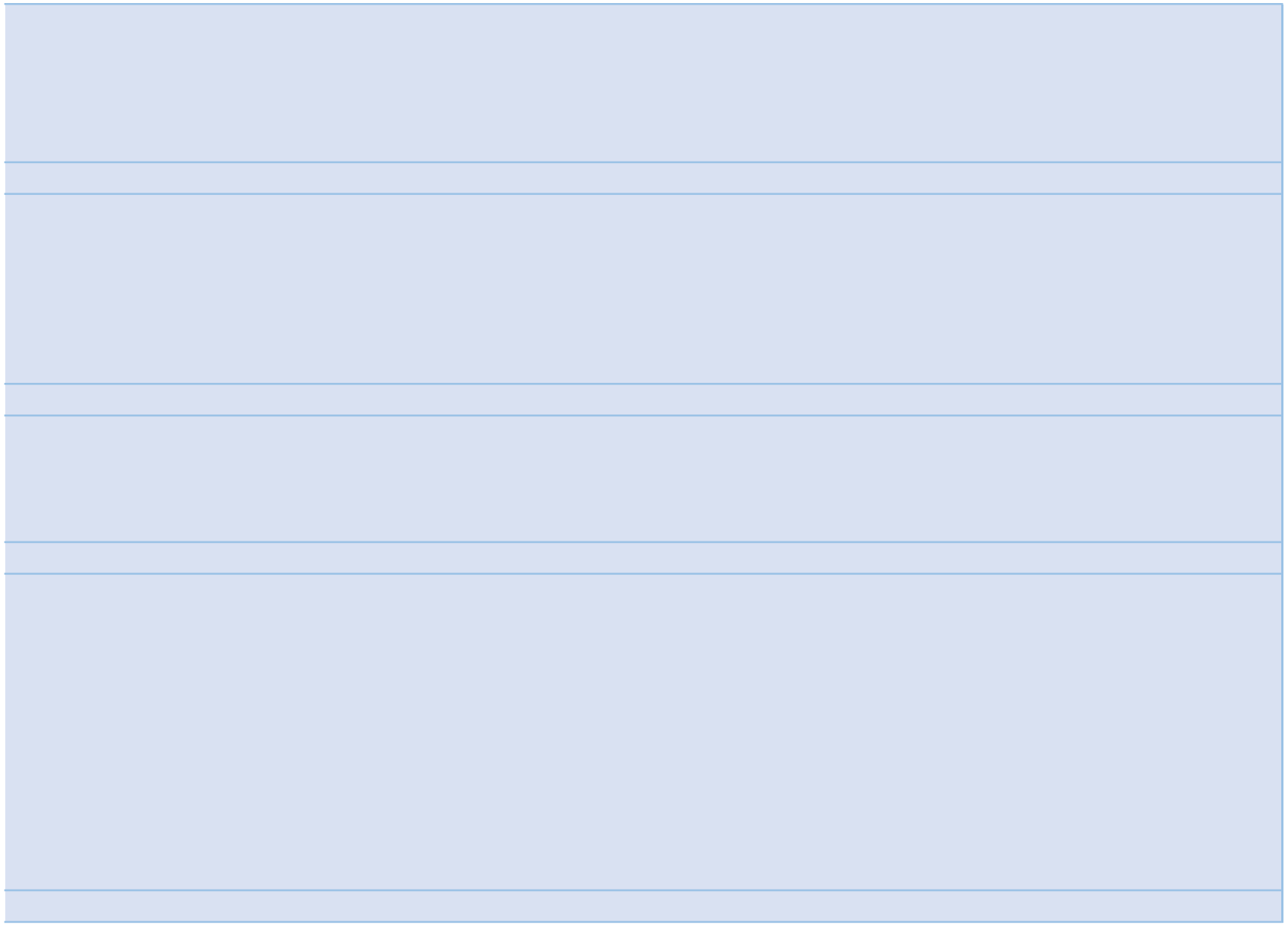


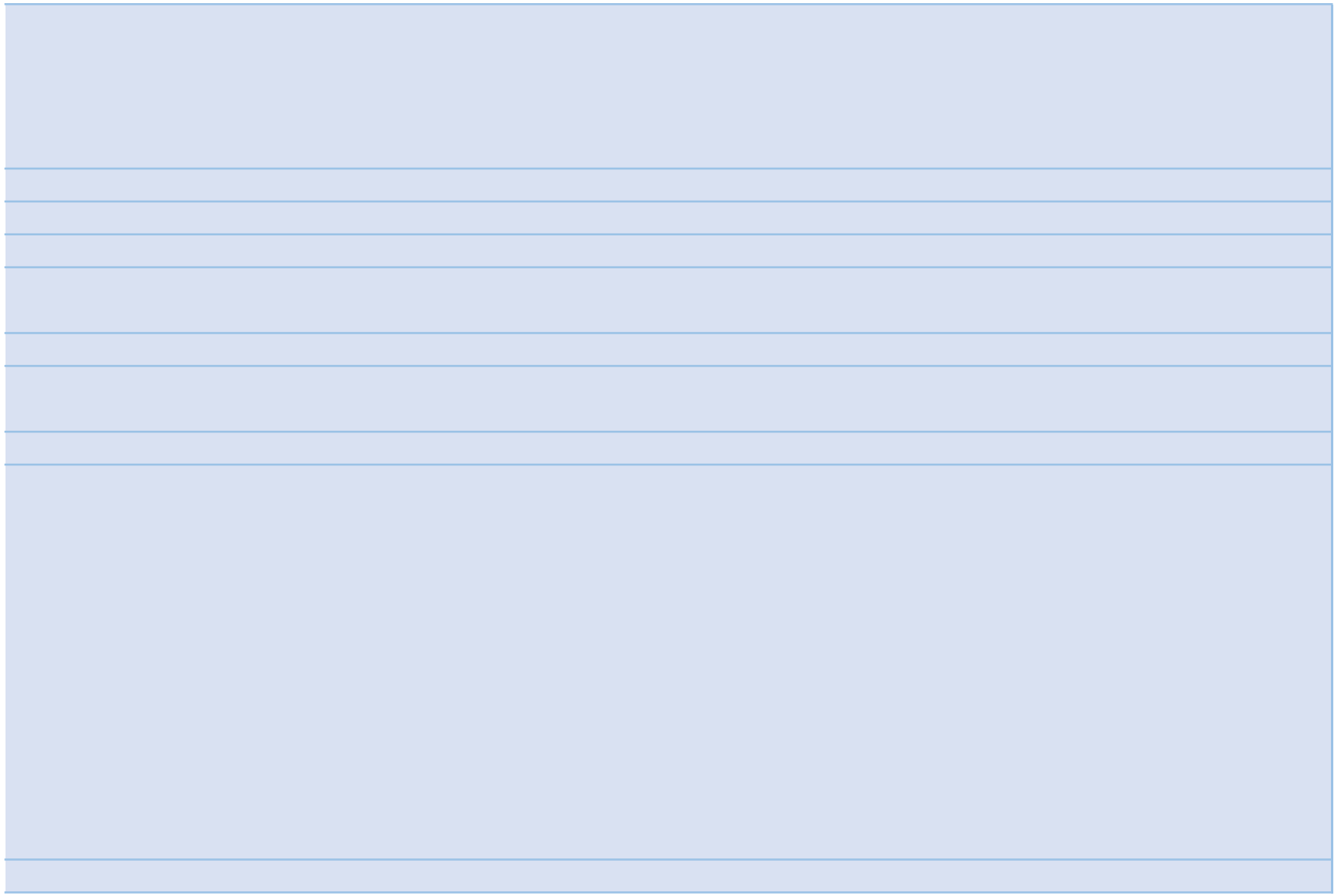


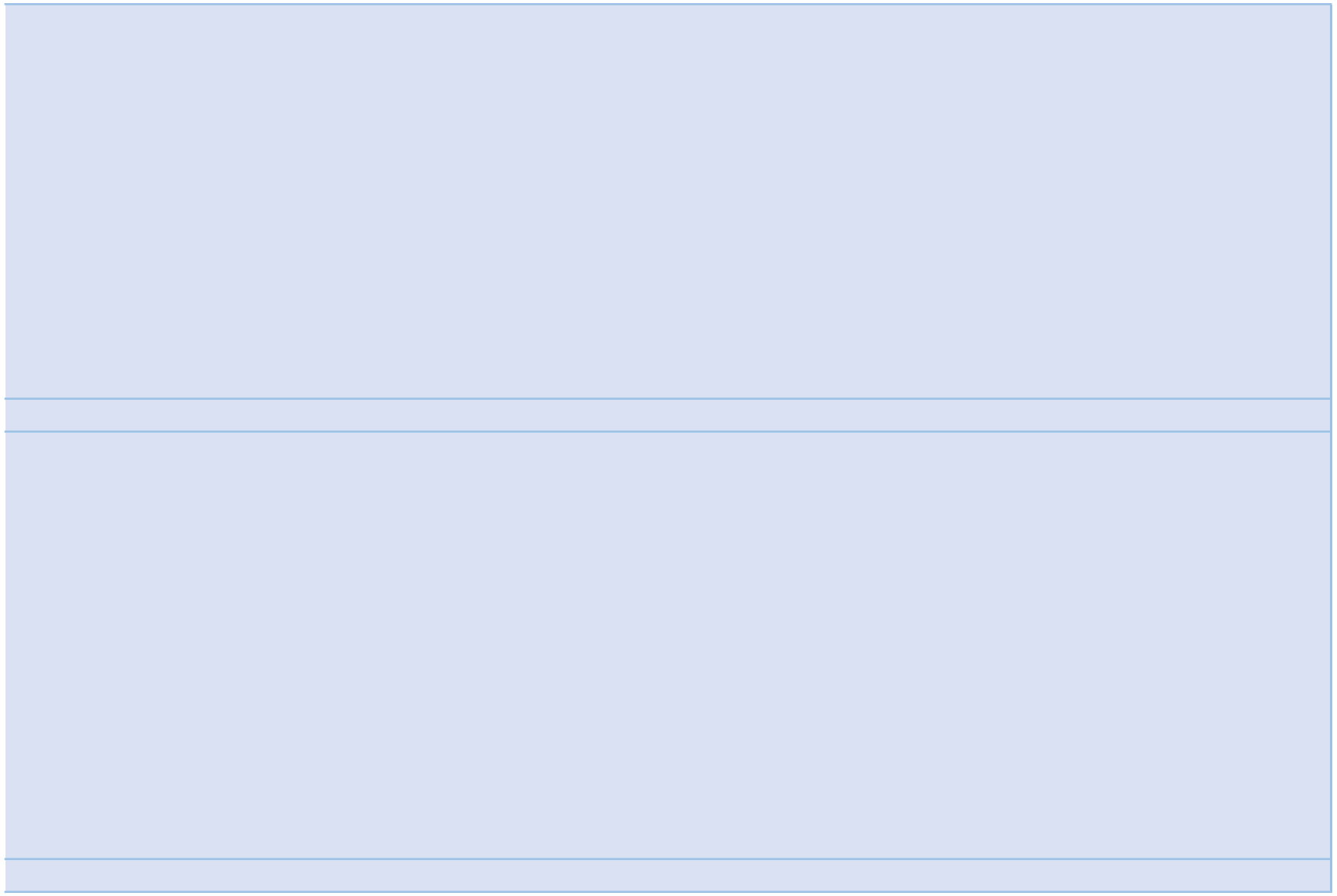


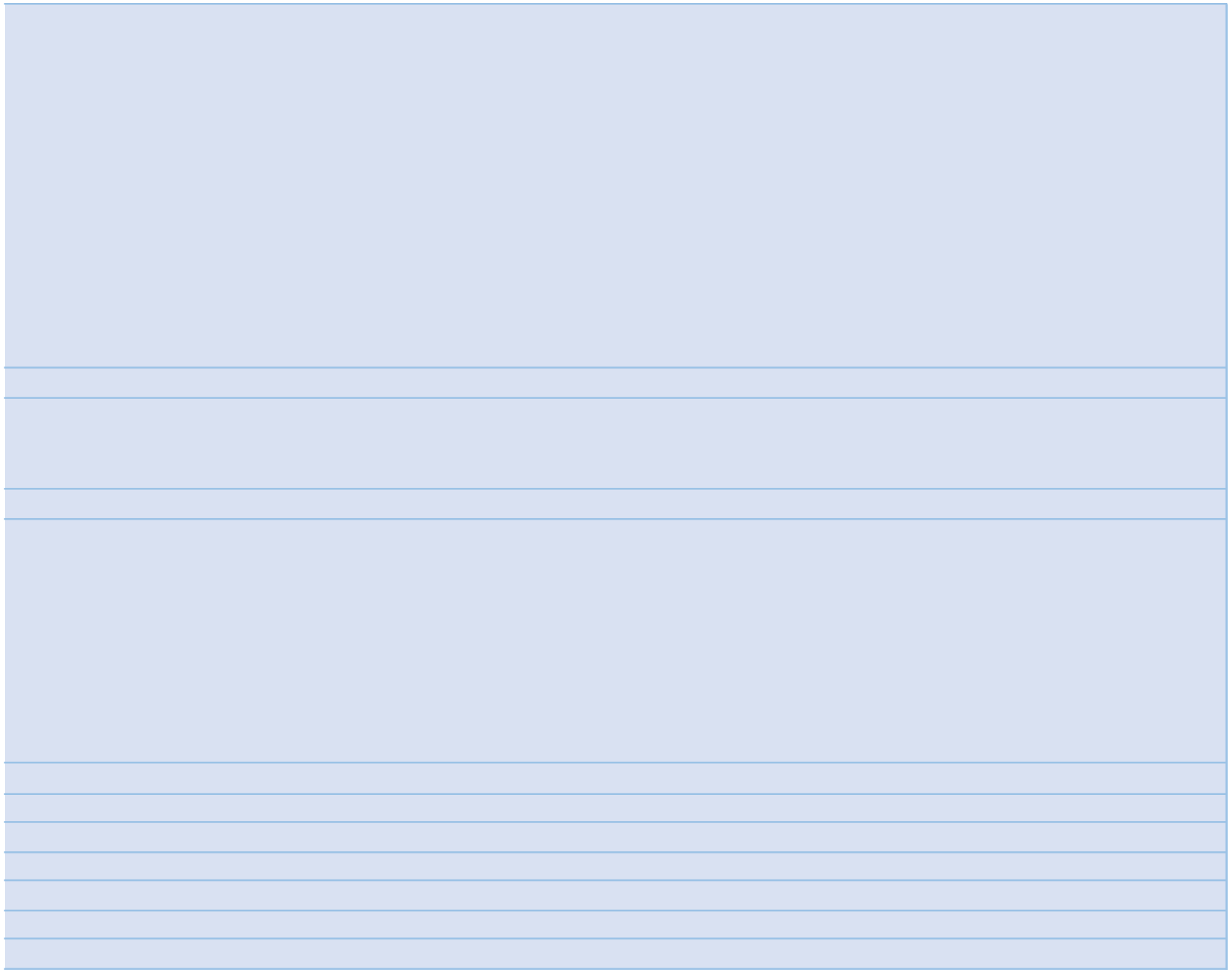


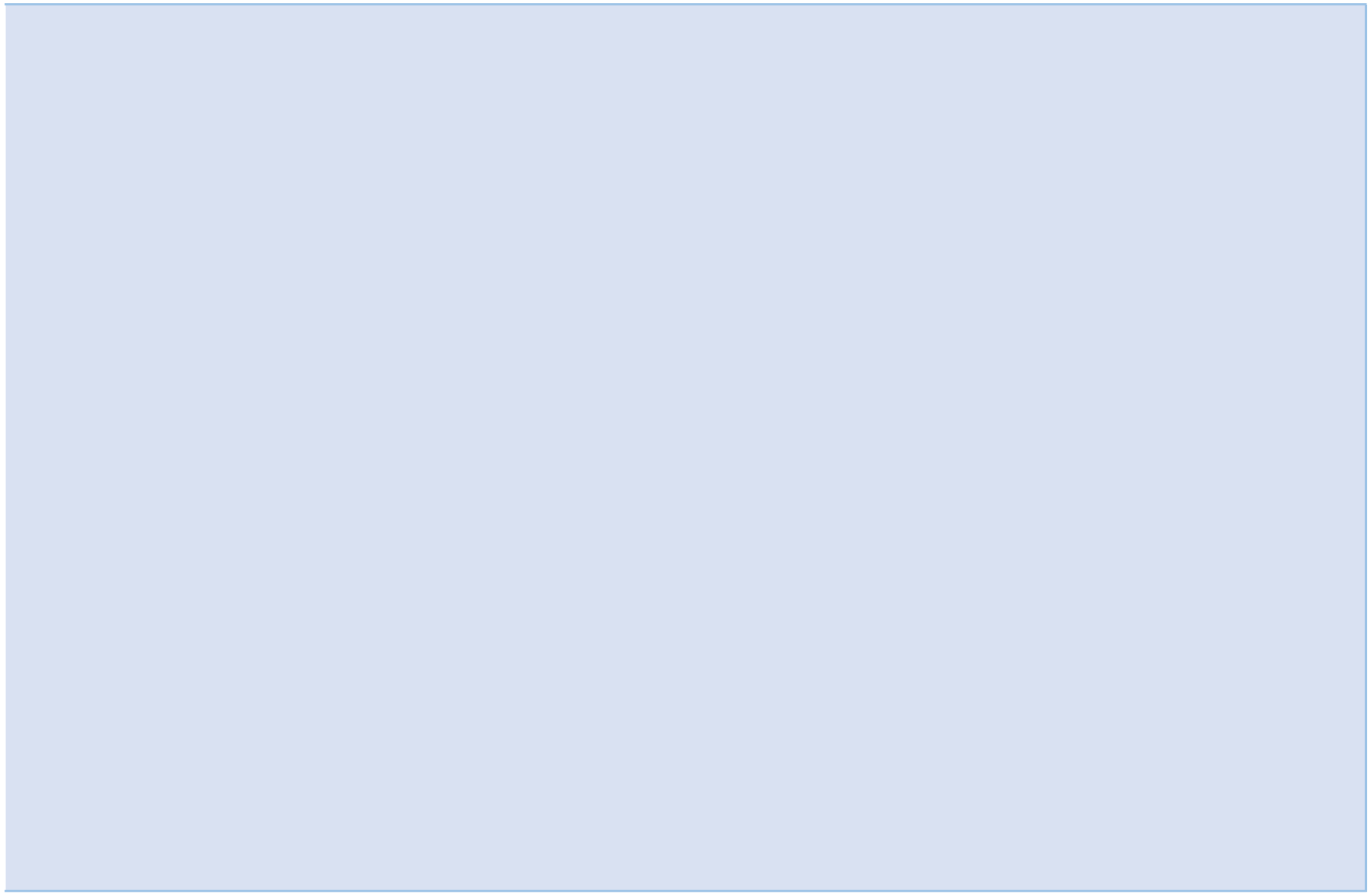


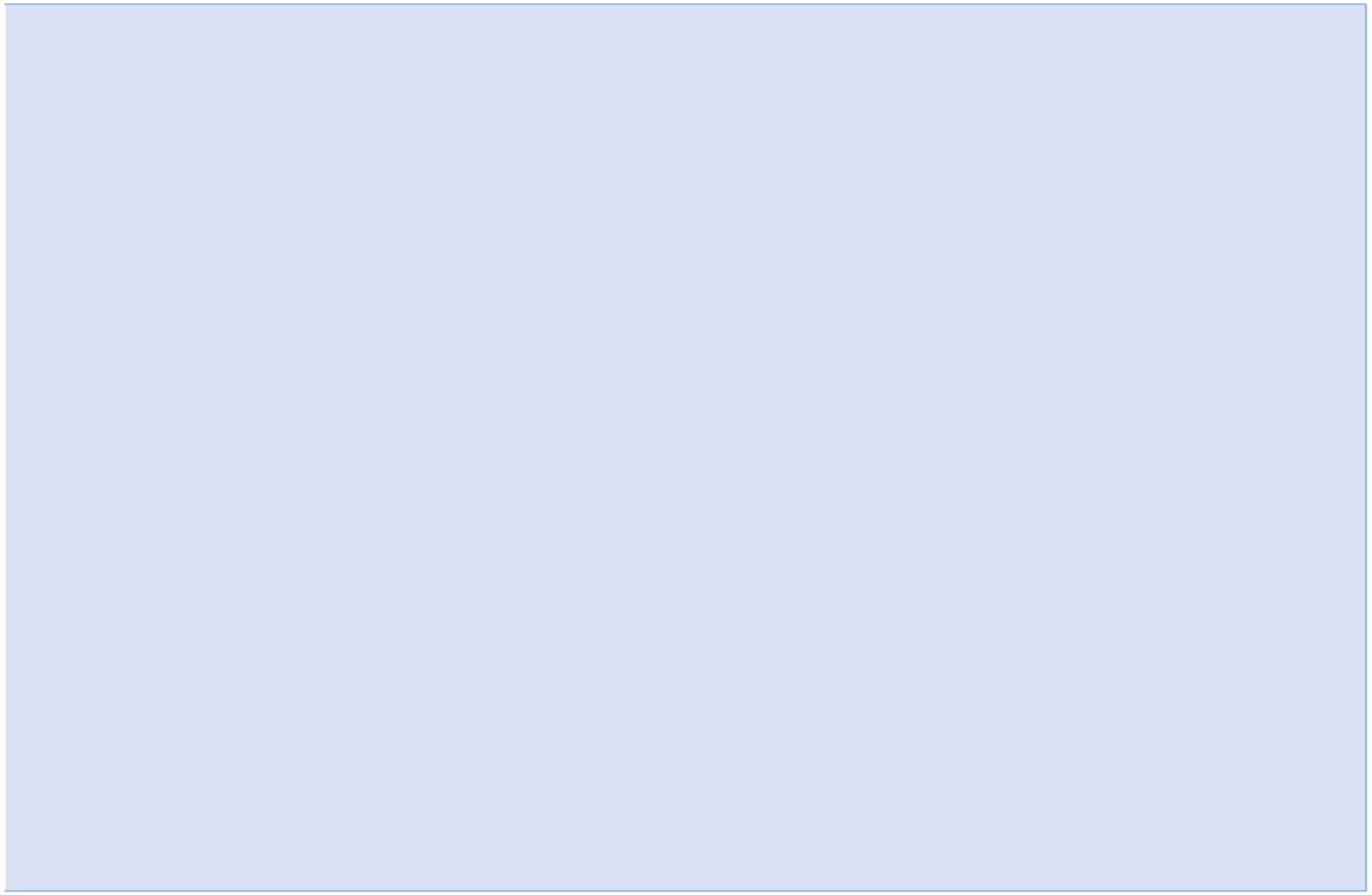


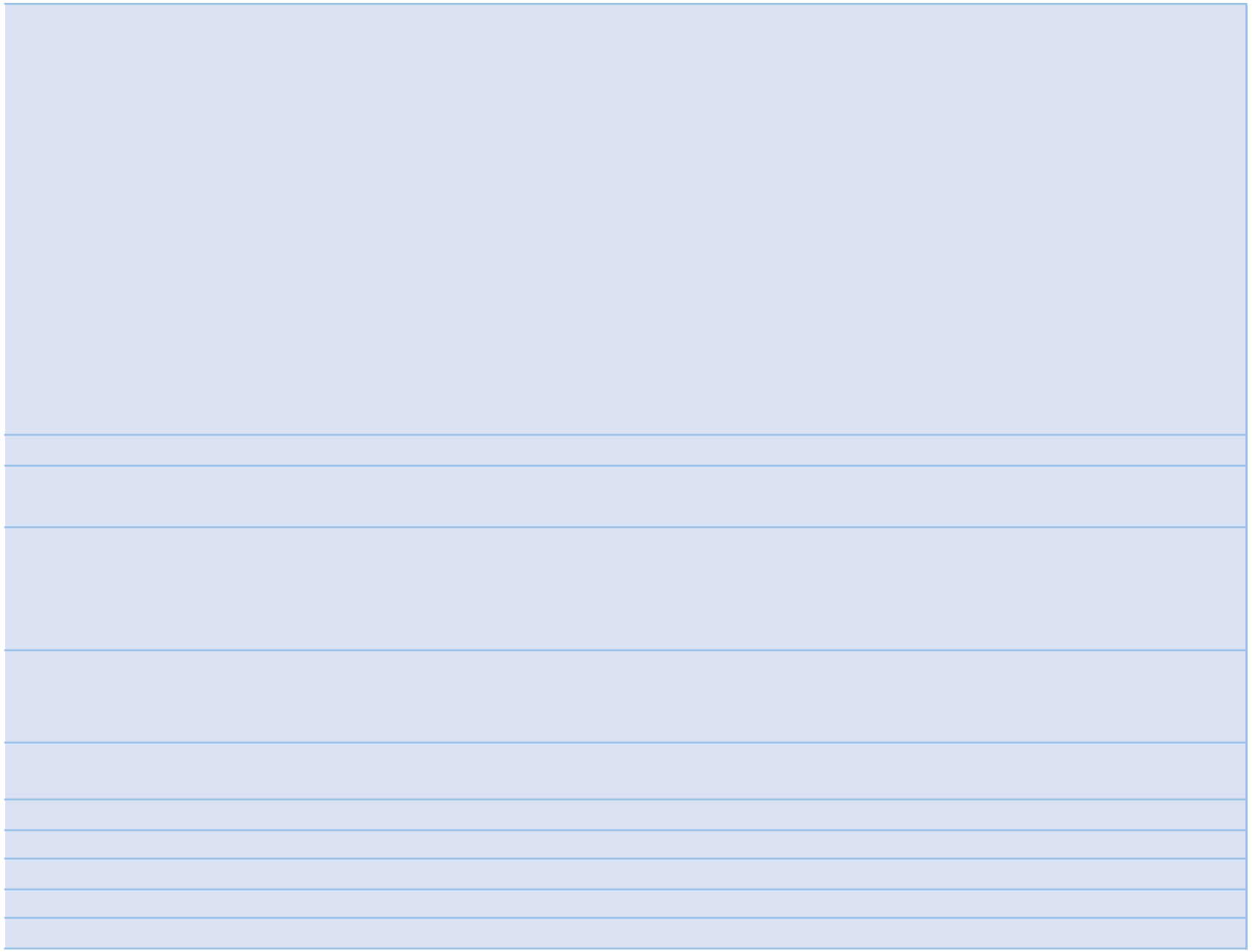


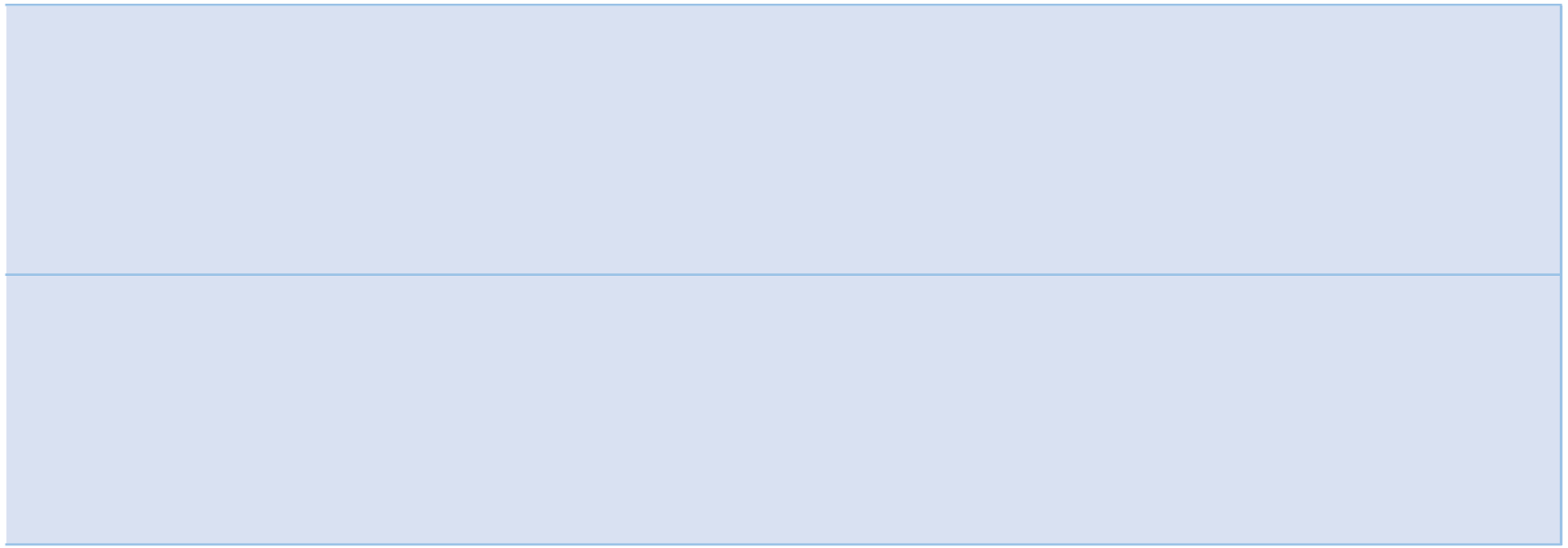


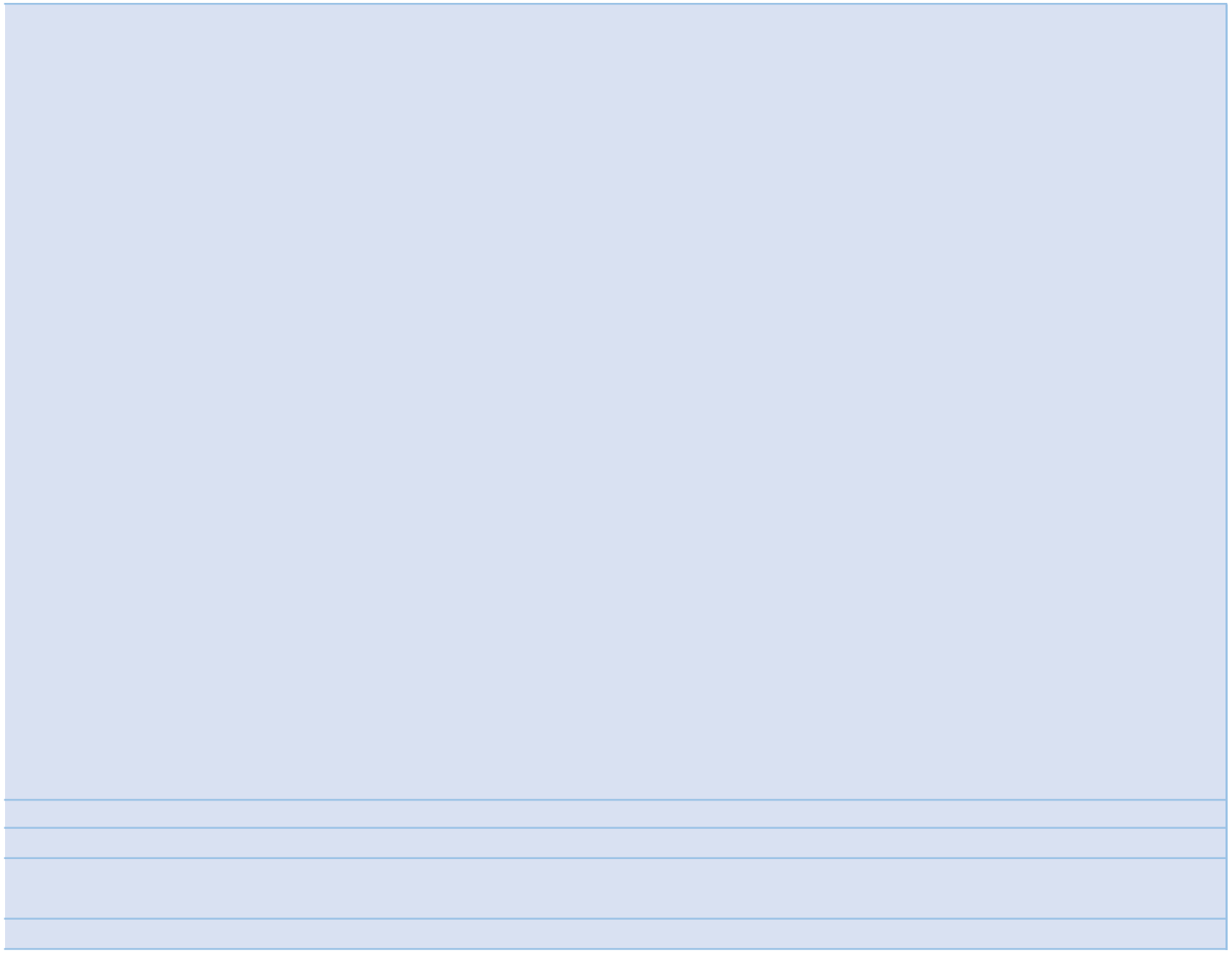








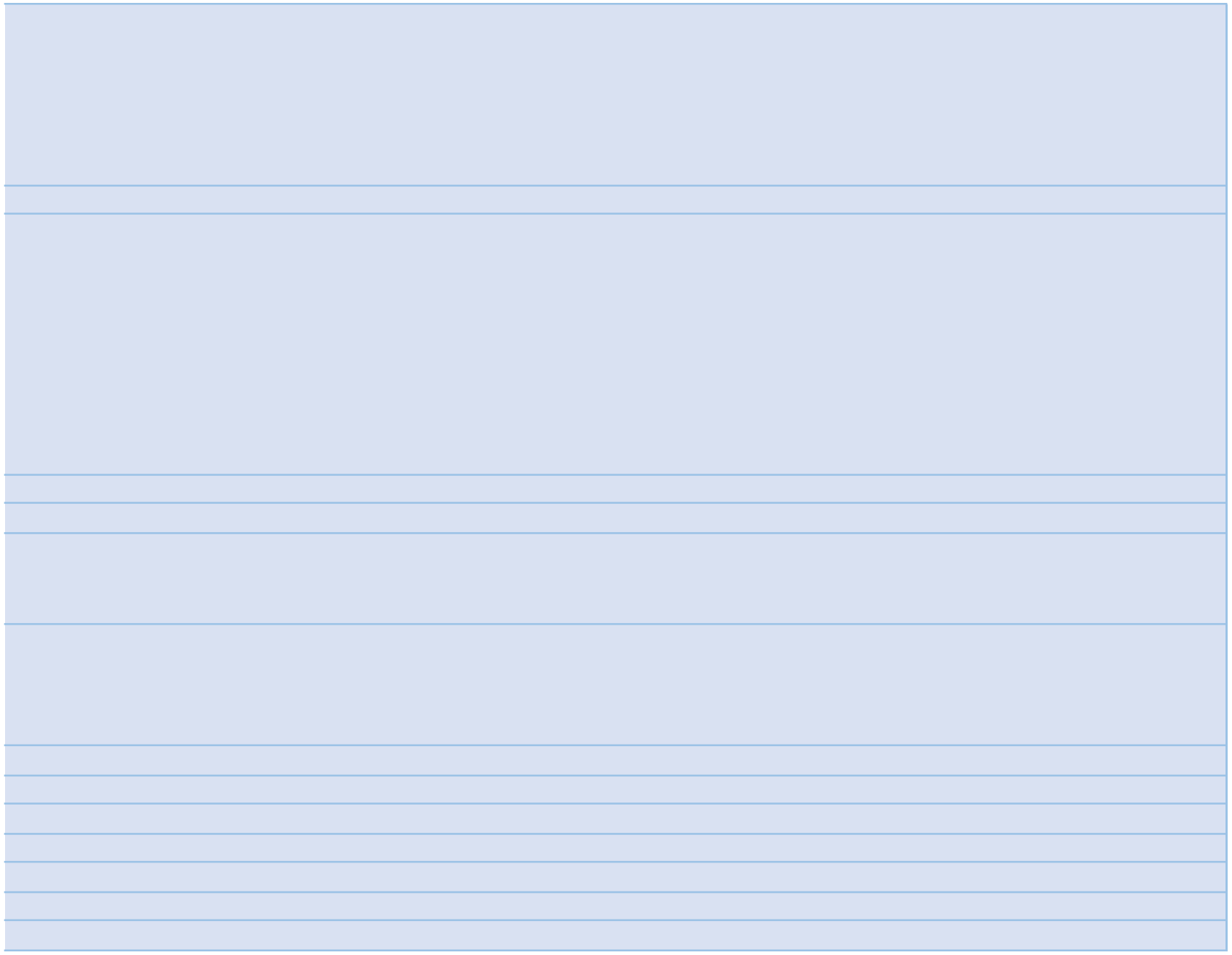


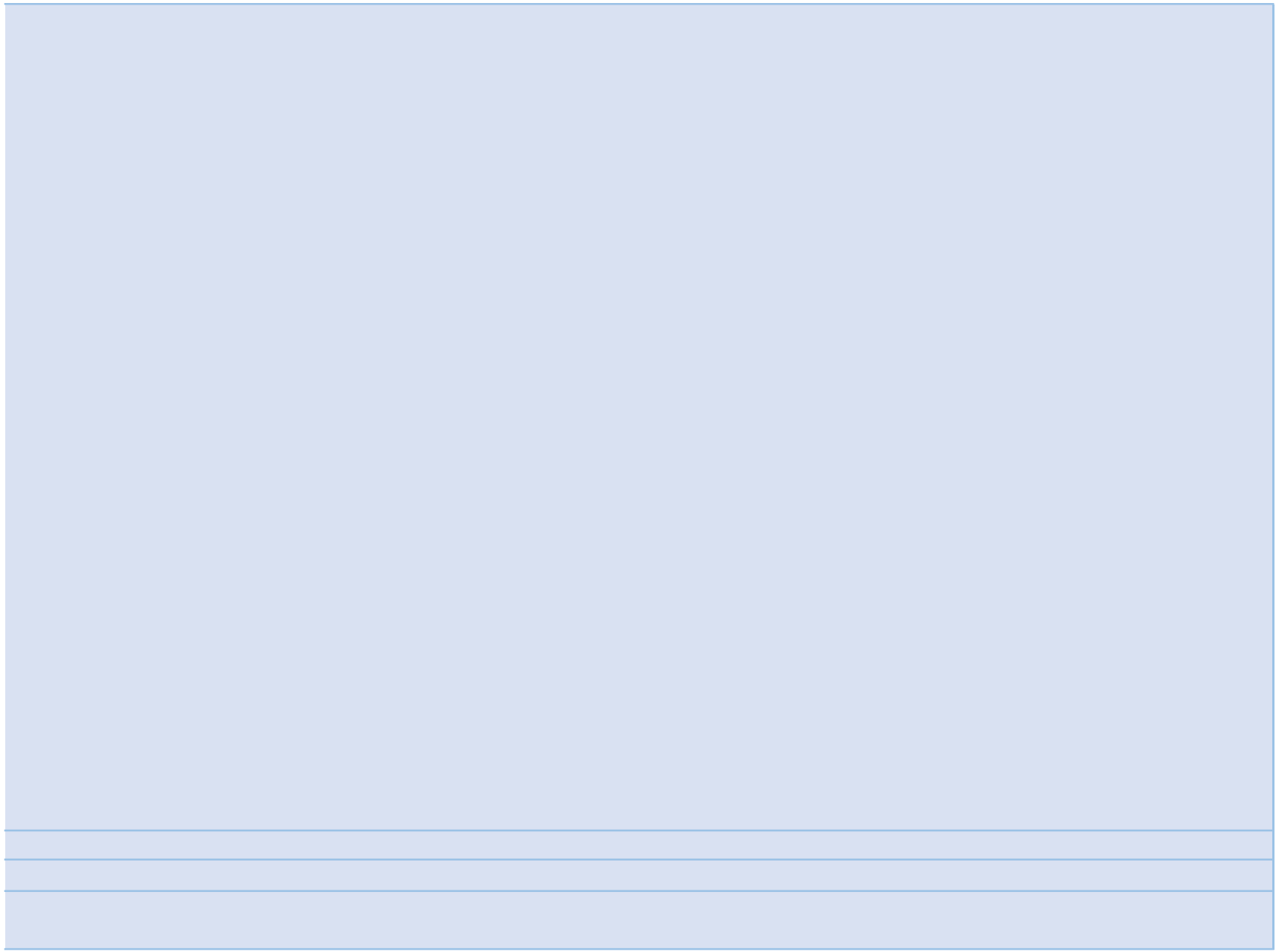


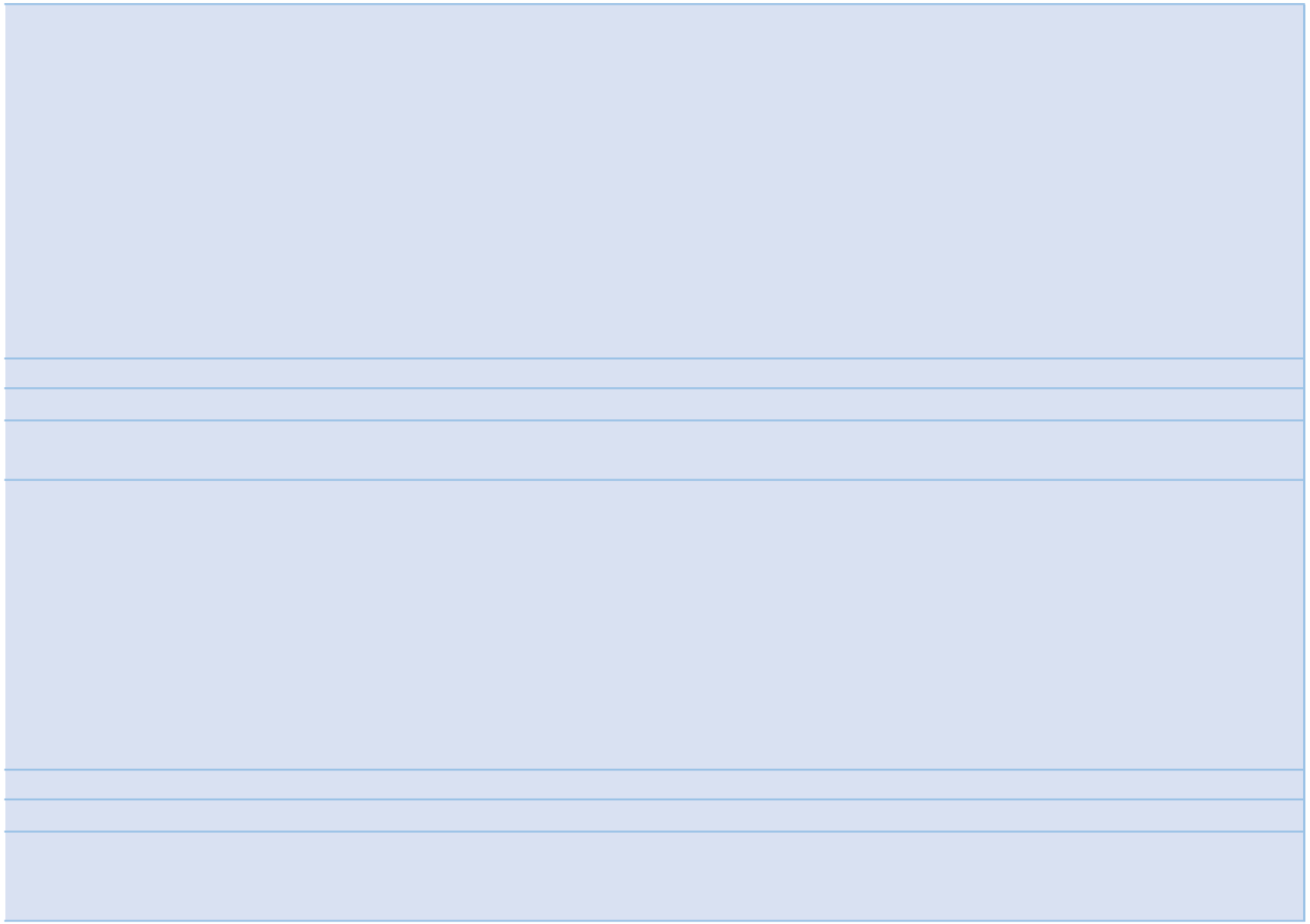
Kristen Lora

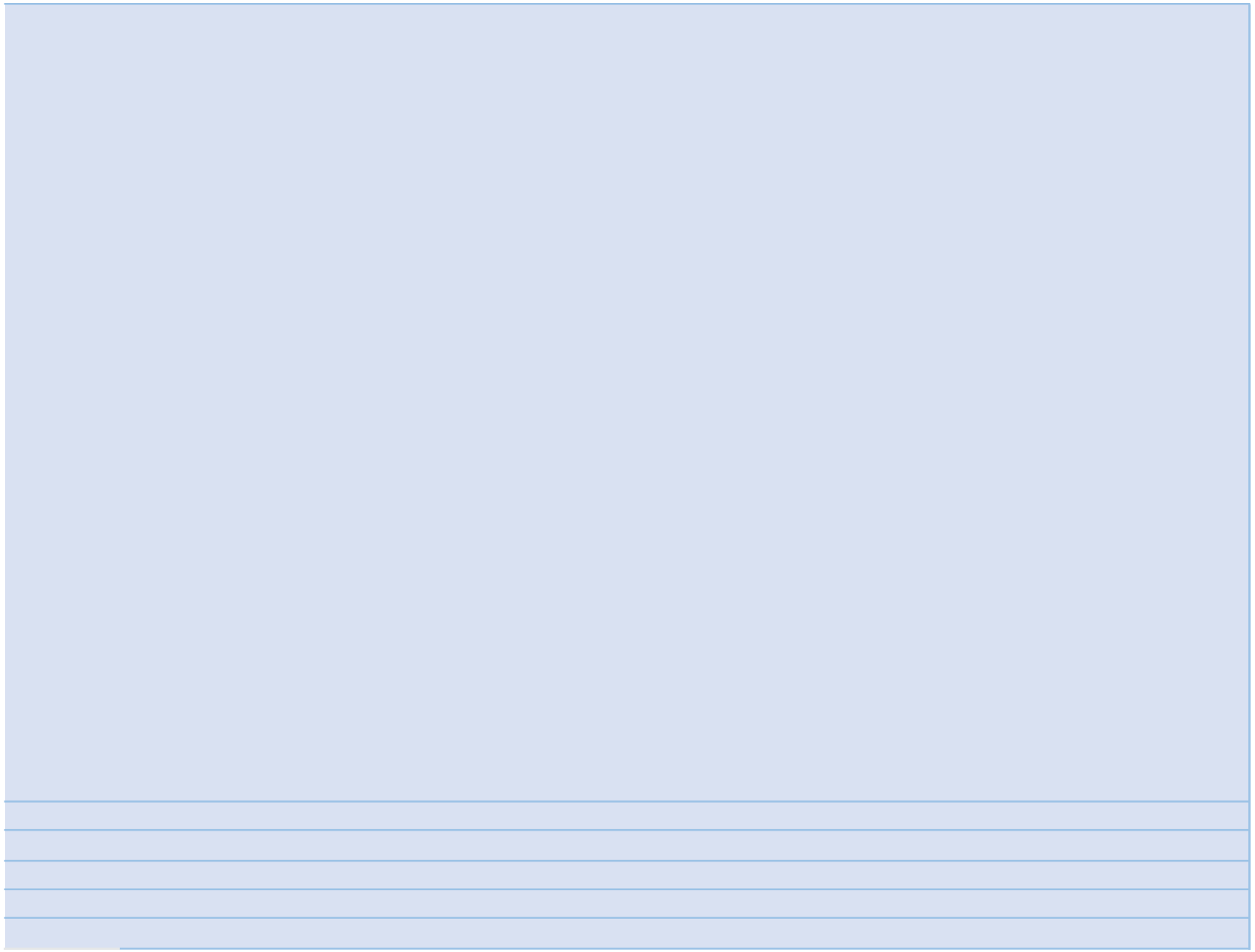
VP of Product

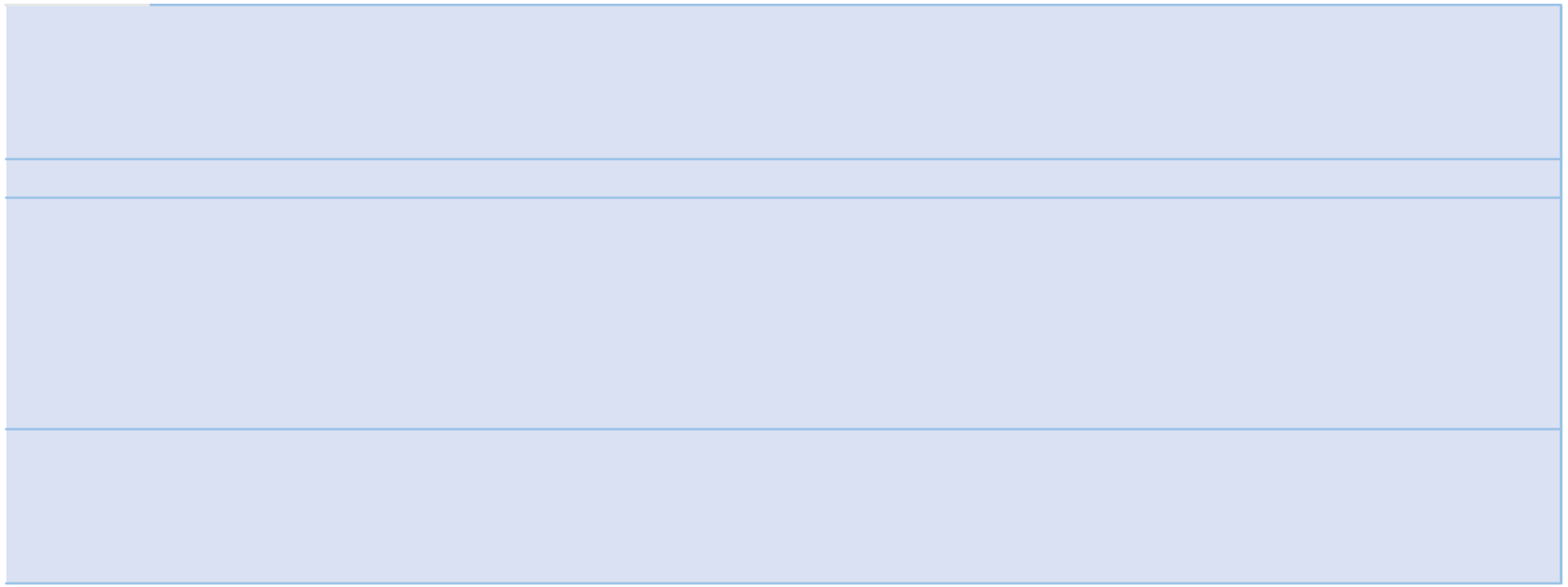
ISACA

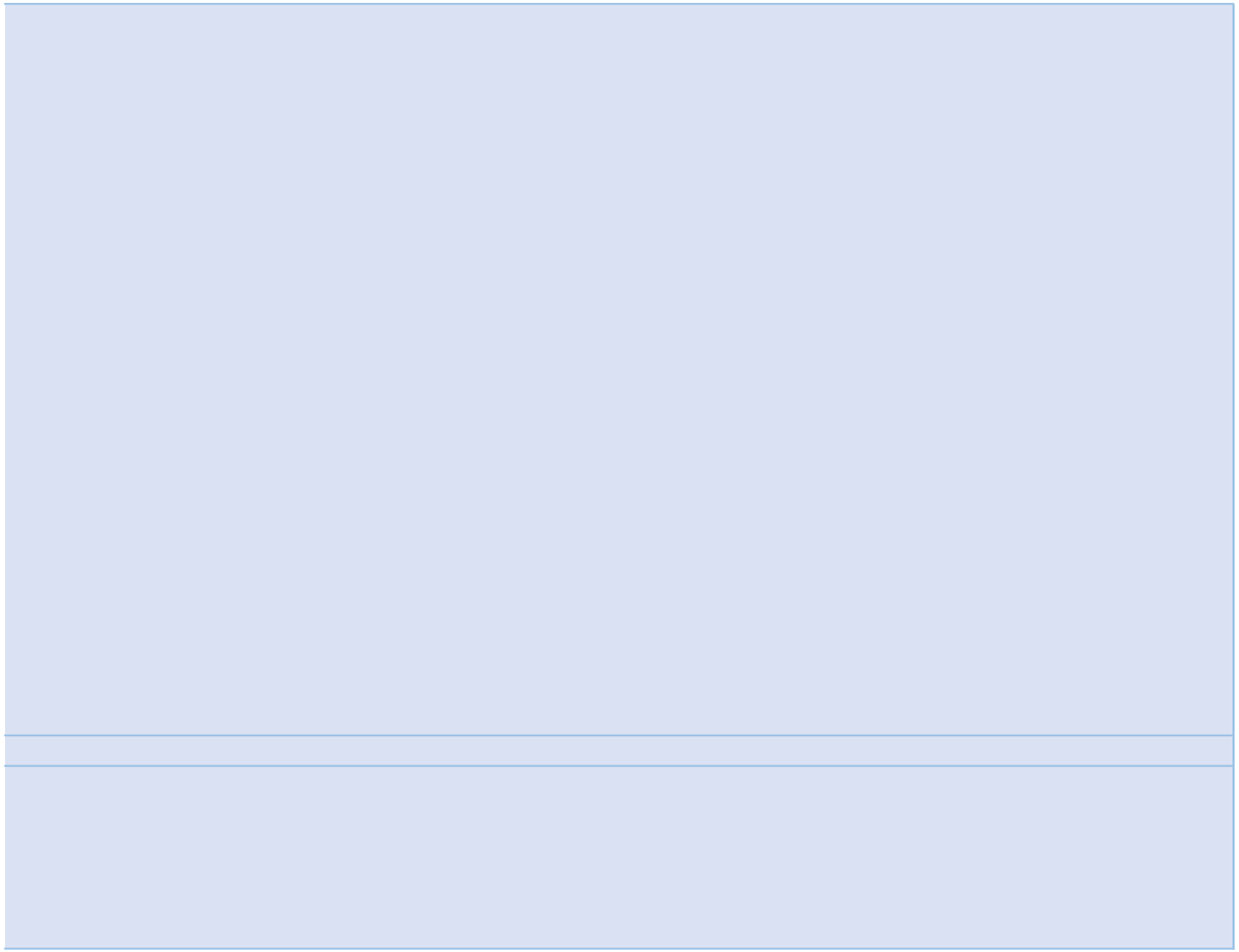


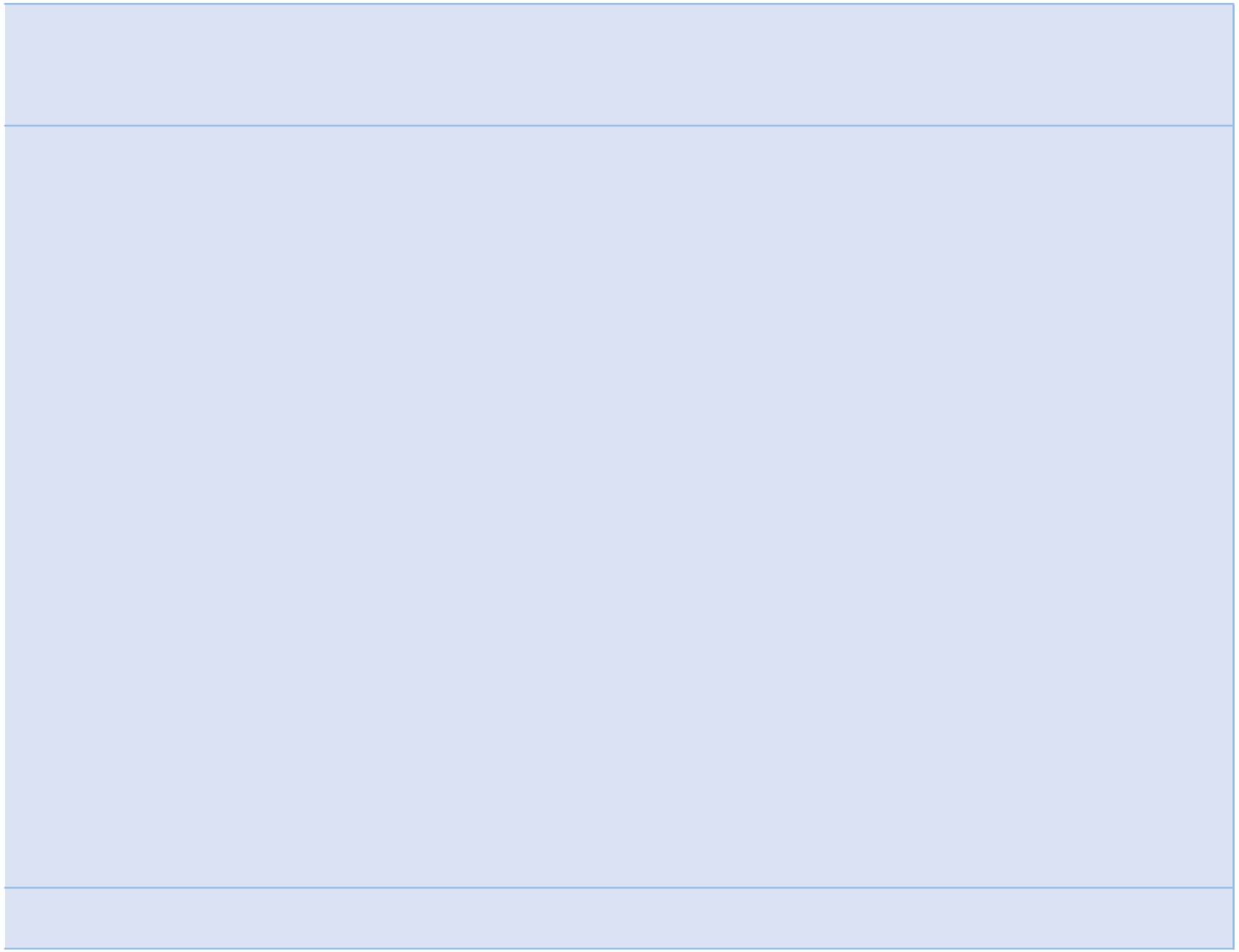


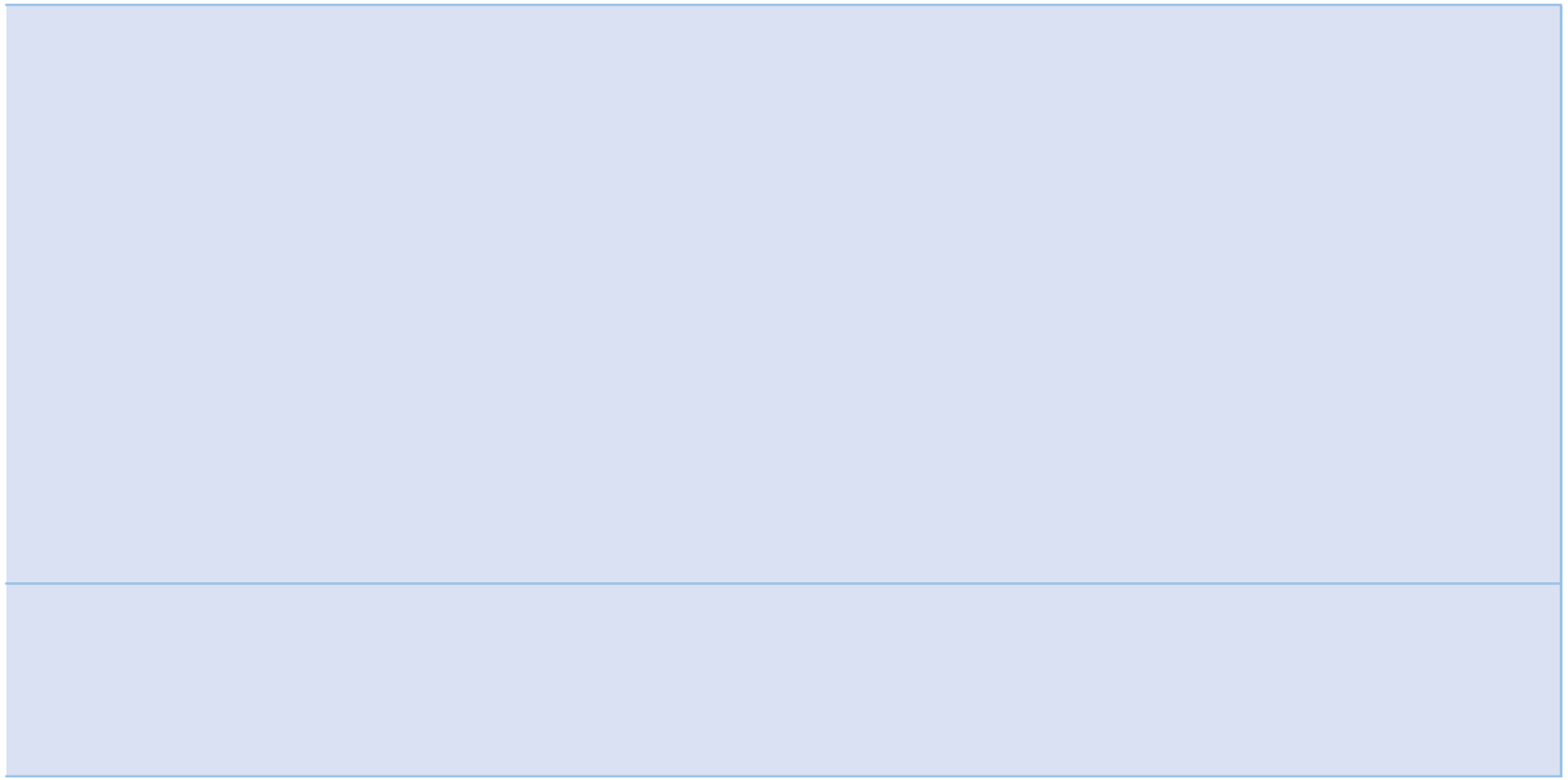


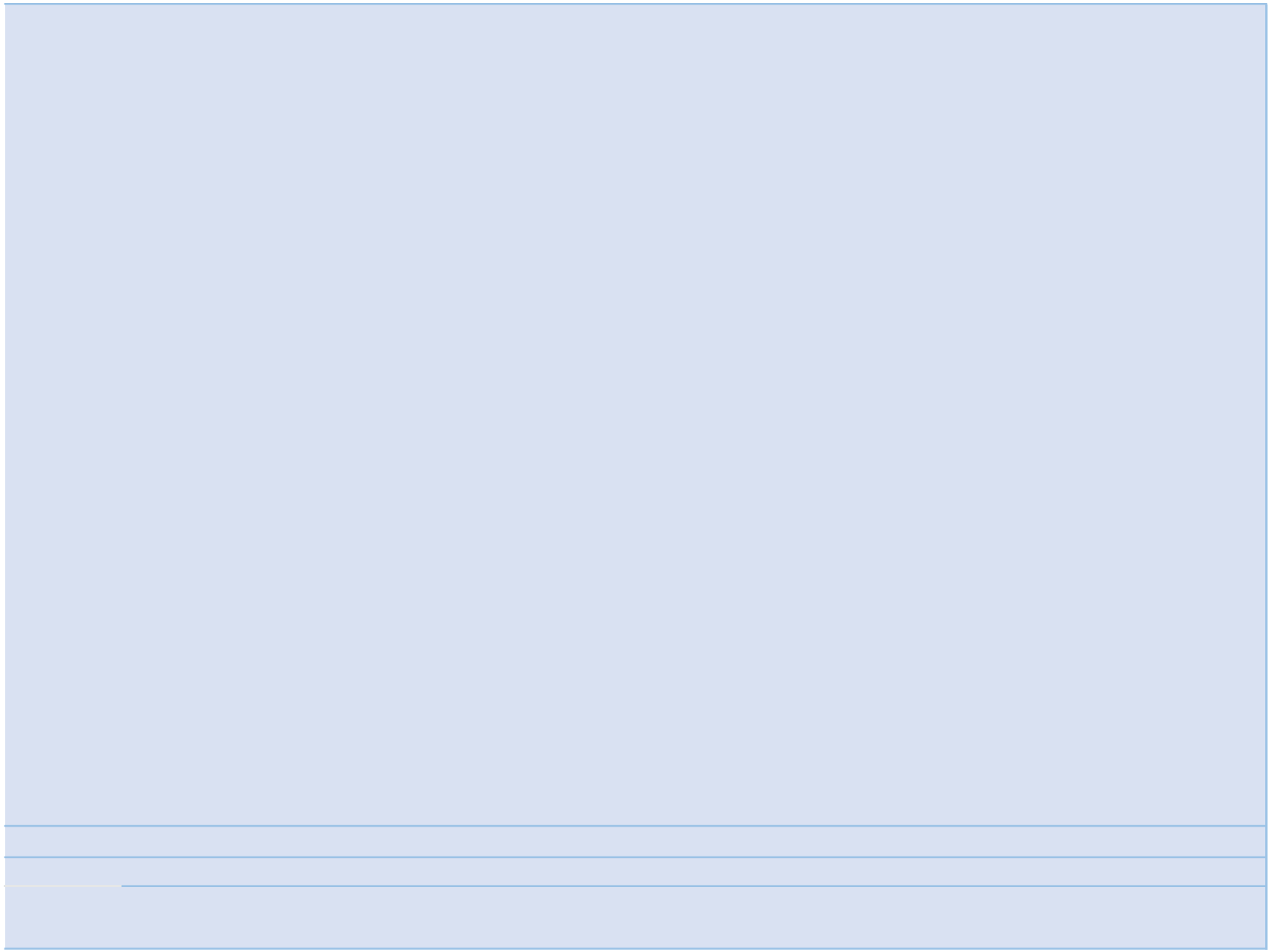


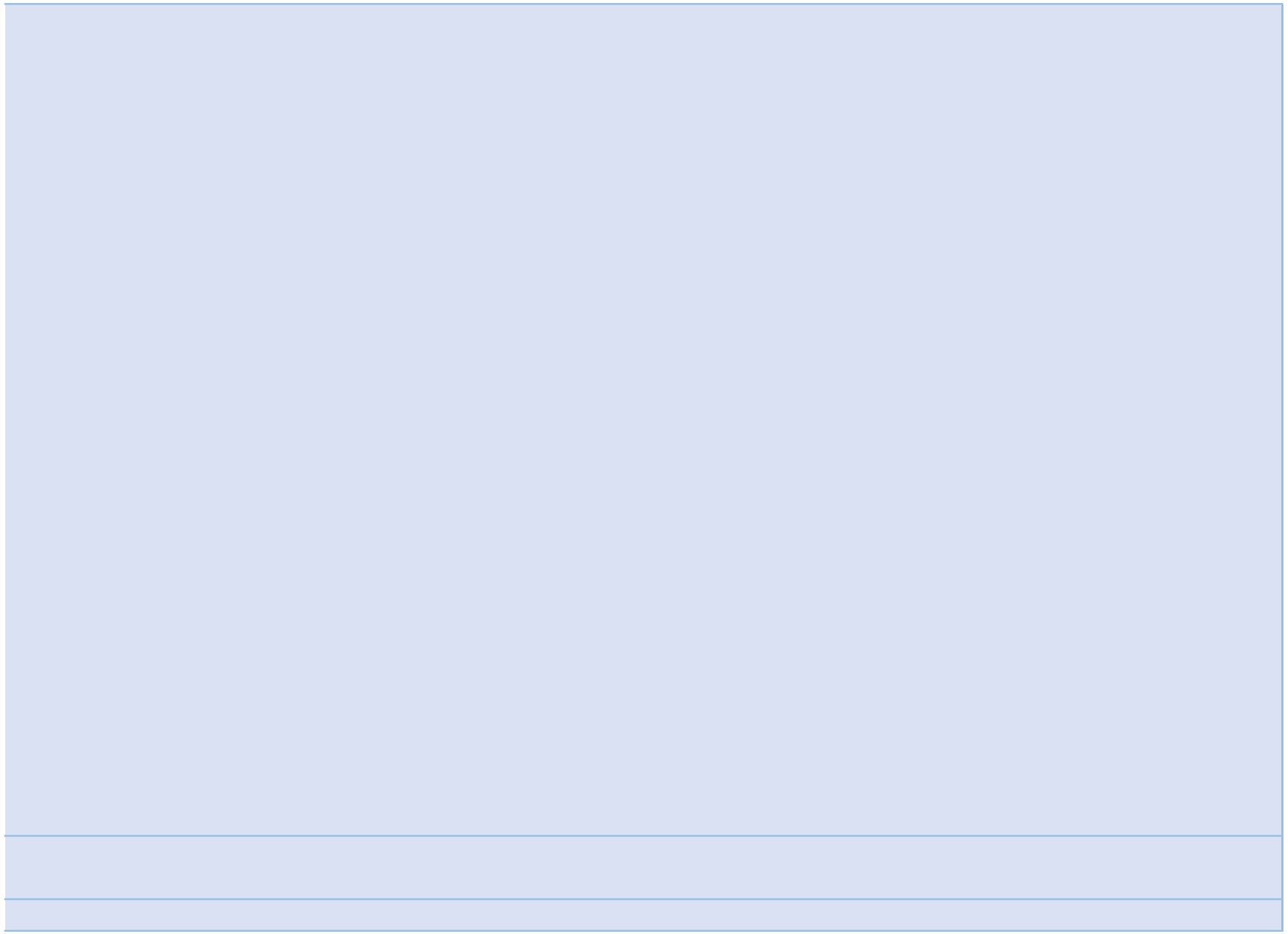












ess. (Aug, 2014).

ıgress. (Sep, 2013).

net Watters. Publisher: Apress. (Dec, 2013).

(Oct, 2019).

lett Publishers. (Nov, 2021).

Schou and Steven Hernandez. Publisher: McGraw-Hill Education. (Sep, 2014).

er: Auerbach Publications. (Mar, 2017).

ug, 2022).

t Learning. (Oct, 2020).

ce Transformation Initiative. (Sep, 2020).

ren Scarfone. (Aug, 2012).

arning. (Oct, 2020).

Apr, 2016).
David Challener. Publisher: Apress. (Jan, 2015).

020).

).

her: Wiley. (Mar, 2015).

ess. (Aug, 2014).

ngress. (Sep, 2013).

2013).

blisher: Apress. (Sep, 2018).

(Oct, 2019).

lett Publishers. (Nov, 2021).

ey J. Haber. Publisher: Apress. (Dec, 2019).

noglu. Publisher: Syngress. (Nov, 2013).

IT. (Nov, 2014).

ress. (Apr, 2016).

t Learning. (Oct, 2020).

en Scarfone. (Aug, 2012).

Mar, 2019).
David Challener. Publisher: Apress. (Jan, 2015).

by Bill Ballad, Tricia Ballad, Erin Banks. Publisher: Jones & Bartlett Learning. (Oct, 2010).

(Jun, 2017).

avis. Publisher: Wiley. (Jan, 2014).

Haber, Brad Hibbert. Publisher: Apress. (Jun, 2018).

ngress. (Sep, 2013).

ns. (Oct, 2018).

fication. (Aug, 2018).

net Watters. Publisher: Apress. (Dec, 2013).

(Sep, 2011).

(Oct, 2019).

Program, 3rd Ed. by Toni Rice. Publisher: SAFECode. (Mar, 2018).

lett Publishers. (Nov, 2021).

ncil of the European Union. (May, 2016).

noglu. Publisher: Syngress. (Nov, 2013).

rey J. Haber. Publisher: Apress. (Dec, 2019).

Schou and Steven Hernandez. Publisher: McGraw-Hill Education. (Sep, 2014).

er: Auerbach Publications. (Mar, 2017).

Press. (Apr, 2016).

Publisher: McGraw-Hill Education. (Oct, 2019).

t Learning. (Oct, 2020).

. Publisher: Packt Publishing. (Aug, 2018).

18).

2012).

e Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).

9).

ce Transformation Initiative. (Sep, 2020).

Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, Mary F. Theofanos. (Jun, 2017).

ul Wouters. Publisher: NIST. (Jun, 2020).

stine. (Dec, 2014).

).

puppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).

lister, Tim Grance, Karen Scarfone. (Apr, 2010).

on, Kelley Dempsey, Ron Ross, Sarbari Gupta, Dennis Bailey. (Aug, 2011).

zations by Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scho

neering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).

n Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl and Mike Vasquez. Publisher: Wiley. (May, 2019).

Mar, 2019).

018).

arning. (Oct, 2020).

Heinemann. (Jul, 2014).

Abhishek Hingnikar, Yvonne Wilson. Publisher: Apress. (Nov, 2022).

Apr, 2016).

7).

Publisher: O'Reilly Media, Inc. (Mar, 2020).

eilly. (Jul, 2017).
, 2018).

avis. Publisher: Wiley. (Jan, 2014).

ngress. (Sep, 2013).

17).

t, Jessi Ashdown. Publisher: O'Reilly Media, Inc. (Mar, 2021).

ncil of the European Union. (May, 2016).

lents by Erdal Ozkaya. Publisher: Packt Publishing. (Feb, 2021).

ul Hoffman. (Jan, 2011).

).

Mar, 2019).

unnar Peterson, Mike Rothman, David Mortman. Publisher: Cloud Security Alliance. (Jul, 2017).

y. (Apr, 2019).
: IT Governance Publishing. (Aug, 2019).

. of Commerce. (Feb, 2004).

n, Joan Hash, Pauline Bowen. (Feb, 2006).

2012).

ycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).

Task Force Transformation Initiative. (Mar, 2011).

ce Transformation Initiative. (Sep, 2020).

t Task Force Transformation Initiative. (Jan, 2022).

Initiative. (Sep, 2020).

ories by Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick. (Aug, 2008).

by Stephen D. Quinn, Murugiah Souppaya, Melanie Cook, Karen Scarfone. (Feb, 2018).

tine. (Dec, 2014).

zations by Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scho
ann, et al. Publisher: OWASP. (Jul, 2005).

David Challener. Publisher: Apress. (Jan, 2015).

rin Banks. Publisher: Jones & Bartlett Learning. (Jul, 2013).

(Jun, 2017).

her: Wiley. (Mar, 2015).

2016).

ns. (Oct, 2018).

ning. (Dec, 2019).

ana L. Burley. Publisher: Addison-Wesley Professional. (Dec, 2014).

ning. (Aug, 2013).

ertification. (Jun, 2014).

16).

ach. Publisher: Wiley. (Dec, 2001).

ddison-Wesley Professional. (Aug, 2012).

ycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).

ce Transformation Initiative. (Sep, 2020).

ories by Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick. (Aug, 2008).

tine. (Dec, 2014).

elia Paulsen, Nadya Bartol, Stephany A. Shankles, Rama Moorthy. (Oct, 2012).

blishing. (Jan, 2017).

Rocky Nook. (Feb, 2014).

e Sachs. Publisher: Addison-Wesley Professional. (Jun, 2016).

(Jun, 2017).

ions. (Sep, 2019).

her: Wiley. (Mar, 2015).

ngress. (Sep, 2013).

gie. (Apr, 2017).

014).

ov, 2015).

noglu. Publisher: Syngress. (Nov, 2013).

er: Auerbach Publications. (Apr, 2016)

ch Publications. (Aug, 2013).

e Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).

. (May, 2020) .

en Scarfone. (Aug, 2012).

Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, Mary F. Theofanos. (Jun, 2017).

uppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).

aul Hoffman. (Jan, 2011).

vid Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone. (Jan, 2014).

by PCI Security Standards Council. Publisher: PCI Security Standards Council, LLC. (May, 2018).

018).

oni. Publisher: Wiley. (May, 2013).

unnar Peterson, Mike Rothman, David Mortman. Publisher: Cloud Security Alliance. (Jul, 2017).
. Publisher: Project Management Institute. (Aug, 2021).

hnical Directors. (Sep, 2002).

ormation Assurance Partnership. (Dec, 2017).

2012).

ycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).

Task Force Transformation Initiative. (Mar, 2011).

. (Jul, 2013)

e Transformation Initiative. (Sep, 2020).

stine. (Dec, 2014).

ouppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).

neering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).

on Boyens, Celia Paulsen, Rama Moorthy, Nadya Bartol. (Apr, 2015).
e. Publisher: Project Management Institute. (Aug, 2021).

015).

ngress. (Sep, 2013).

net Watters. Publisher: Apress. (Dec, 2013).

)96).

er: Auerbach Publications. (Apr, 2016)

Graw-Hill Osborne Media. (Aug, 2014)

Publisher: McGraw-Hill Education. (Oct, 2019).

2012).

e Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).

ycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).

Task Force Transformation Initiative. (Mar, 2011).

ce Transformation Initiative. (Sep, 2020).

wanson, Kevin Stine, Nadya Bartol, Anthony Brown, Will Robinson. (Jul, 2008)

en Scarfone. (Aug, 2012).

on, Kelley Dempsey, Ron Ross, Sarbari Gupta, Dennis Bailey. (Aug, 2011).

neering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).

(Apr, 2016).

hem AlFardan. Publisher: Cisco Press. (Nov, 2015).

7).

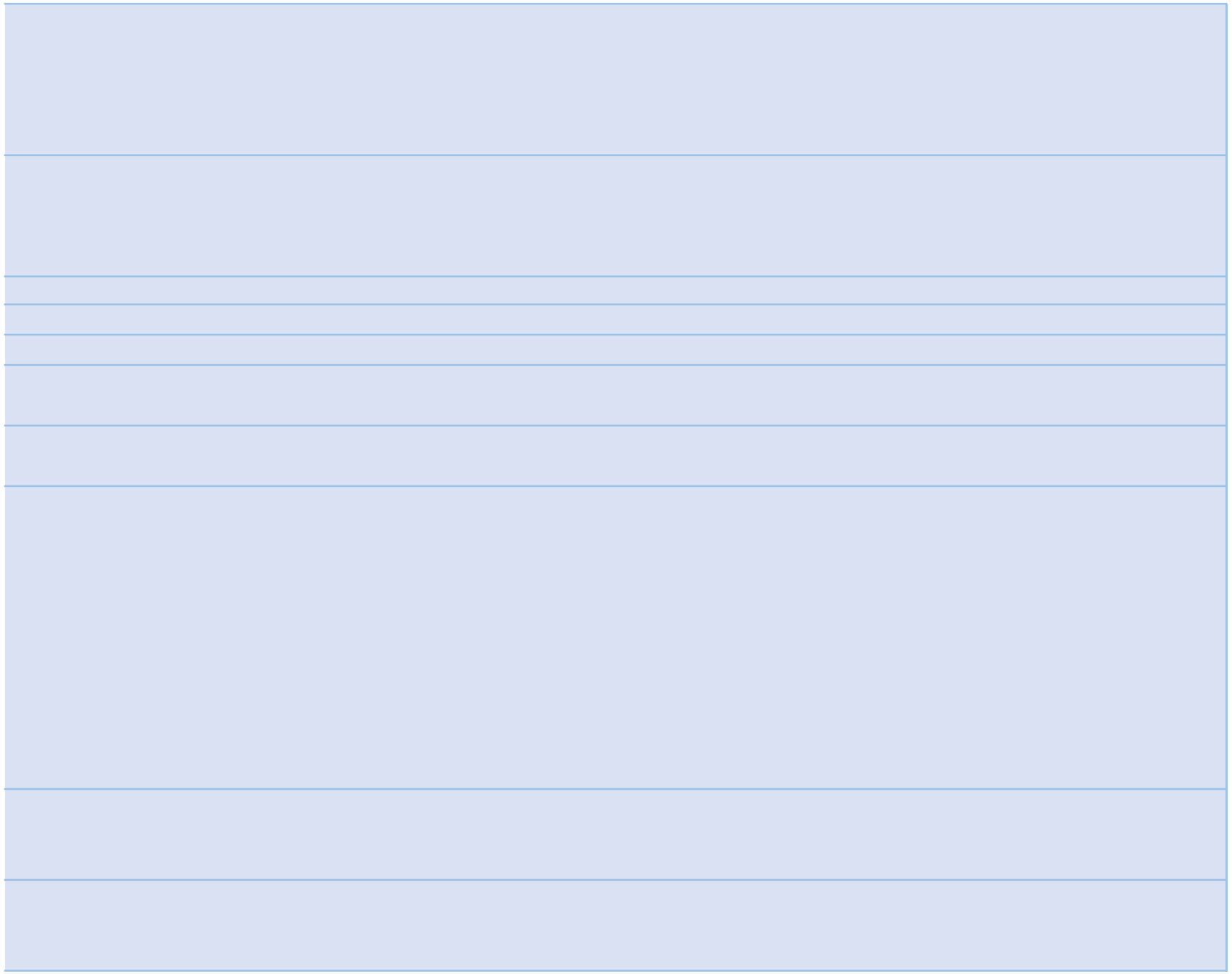
: provides a comprehensive review of the topics covered in the Official ISC2 Training Course and will help you navigate key cybersec

ersecurity. ISC2 is offering free Certified in Cybersecurity (CC) Online Self-Paced Training and an exam to 1 million people as part of

arning supports include:

e and offline.

people entering the cybersecurity workforce without direct IT experience. Getting Certified in Cybersecurity provides employers wit



/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)

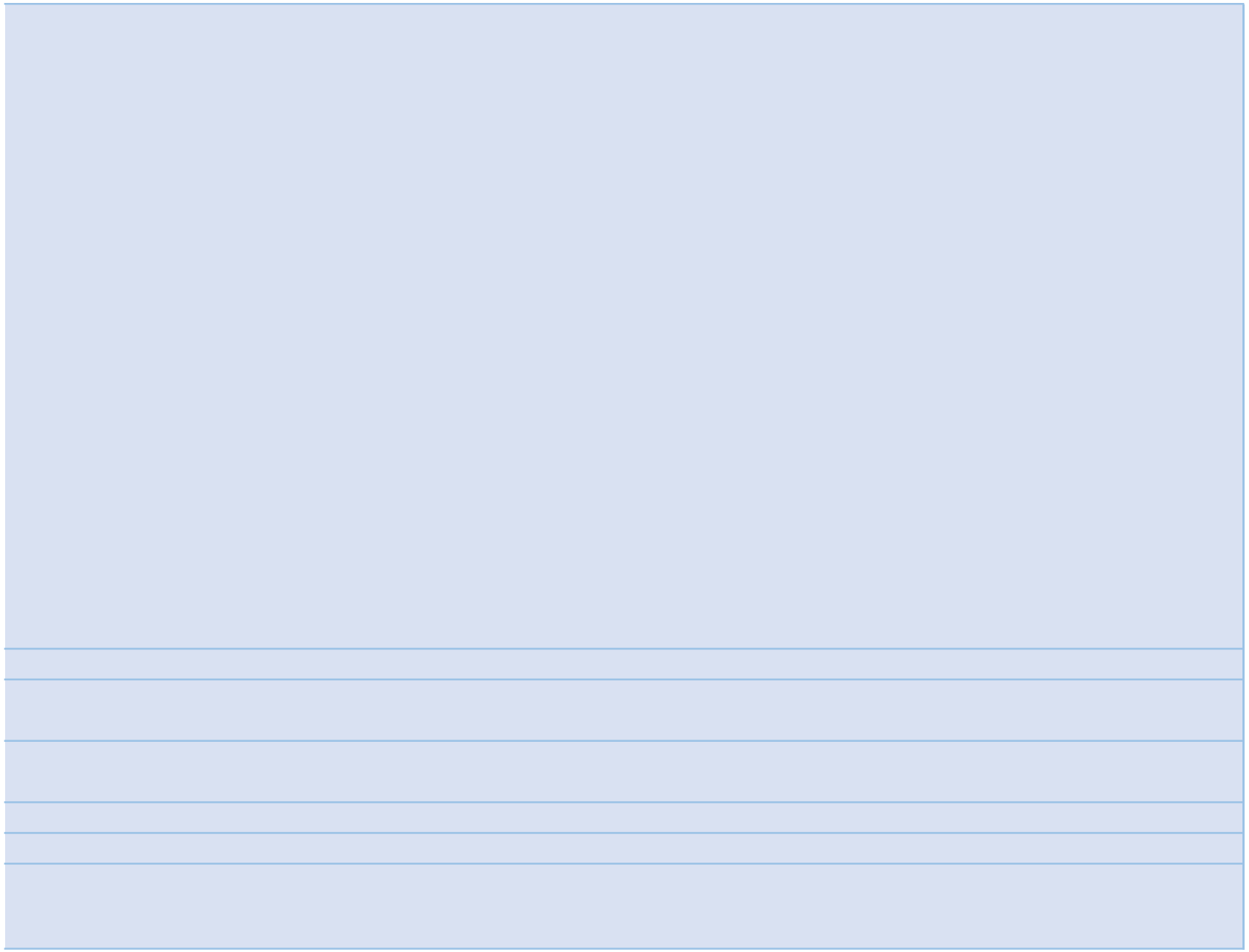
hannel)
ion detection system (NIDS))

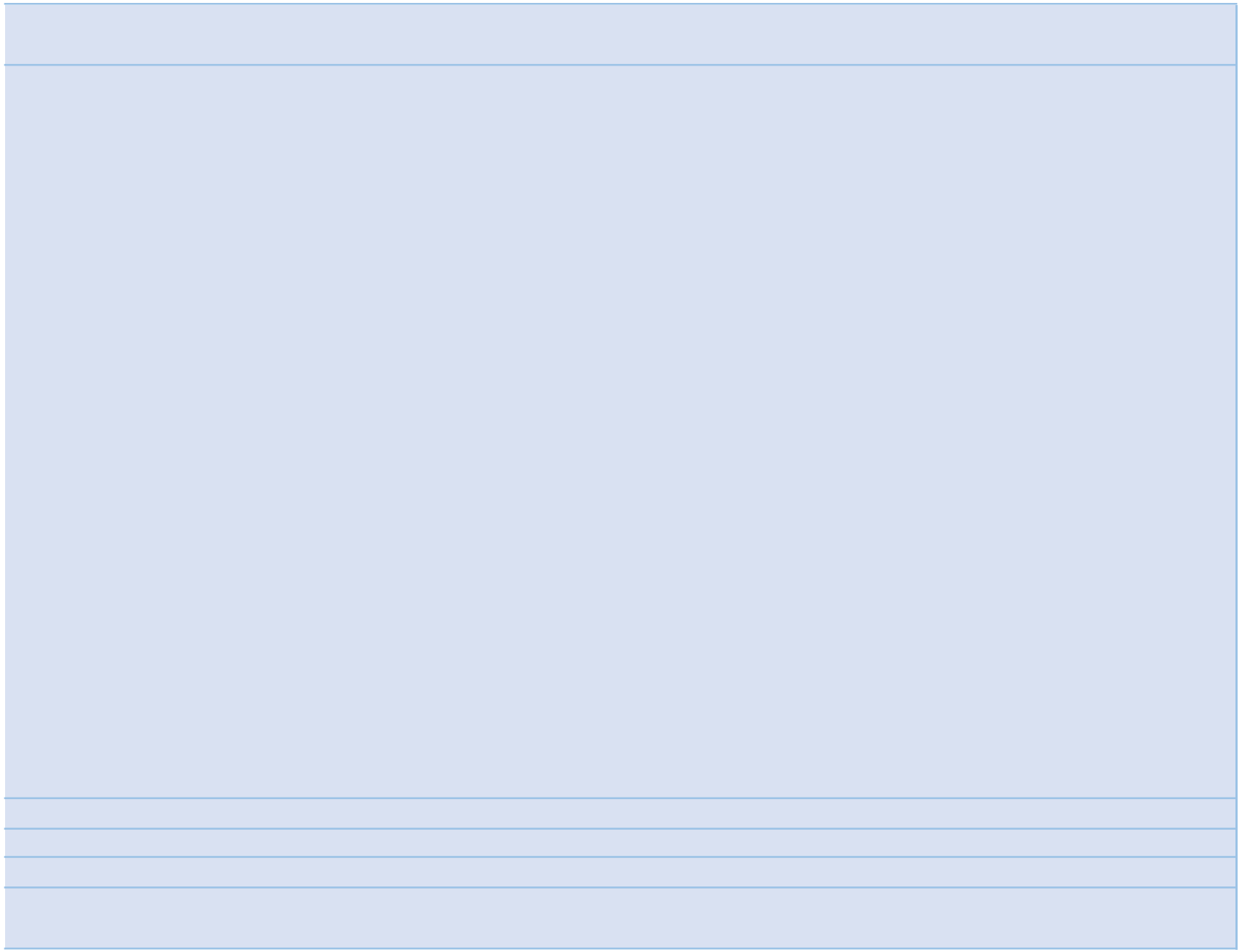
fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
etwork (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Interne
ucture as a Service (IaaS), Platform as a Service (PaaS), hybrid)

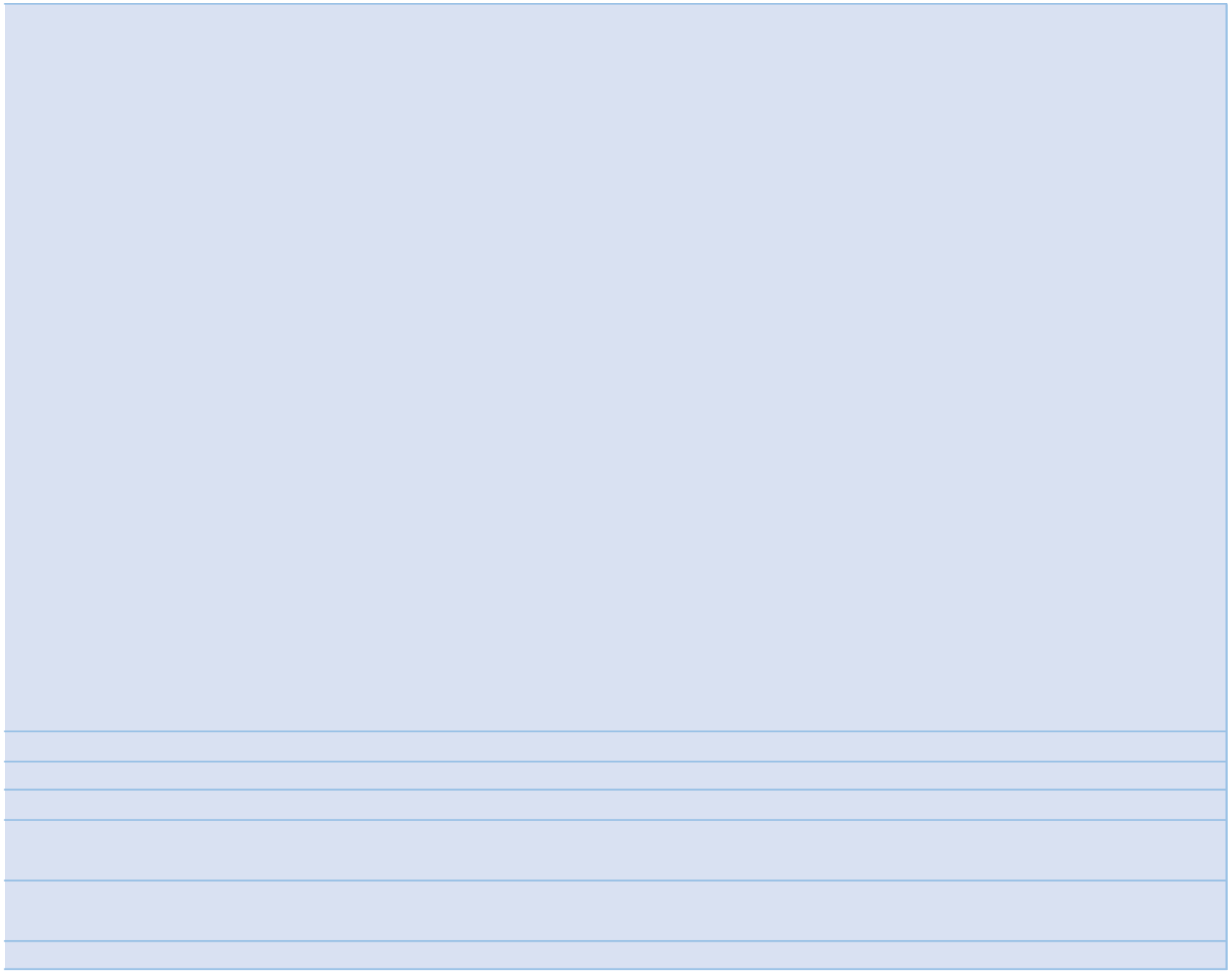
written permission. ISC2, CISSP, SSCP, CCSP, CGRC, CSSLP, HCISPP, ISSAP, ISSEP, ISSMP, CC, and CBK are registered marks of ISC2, Ir

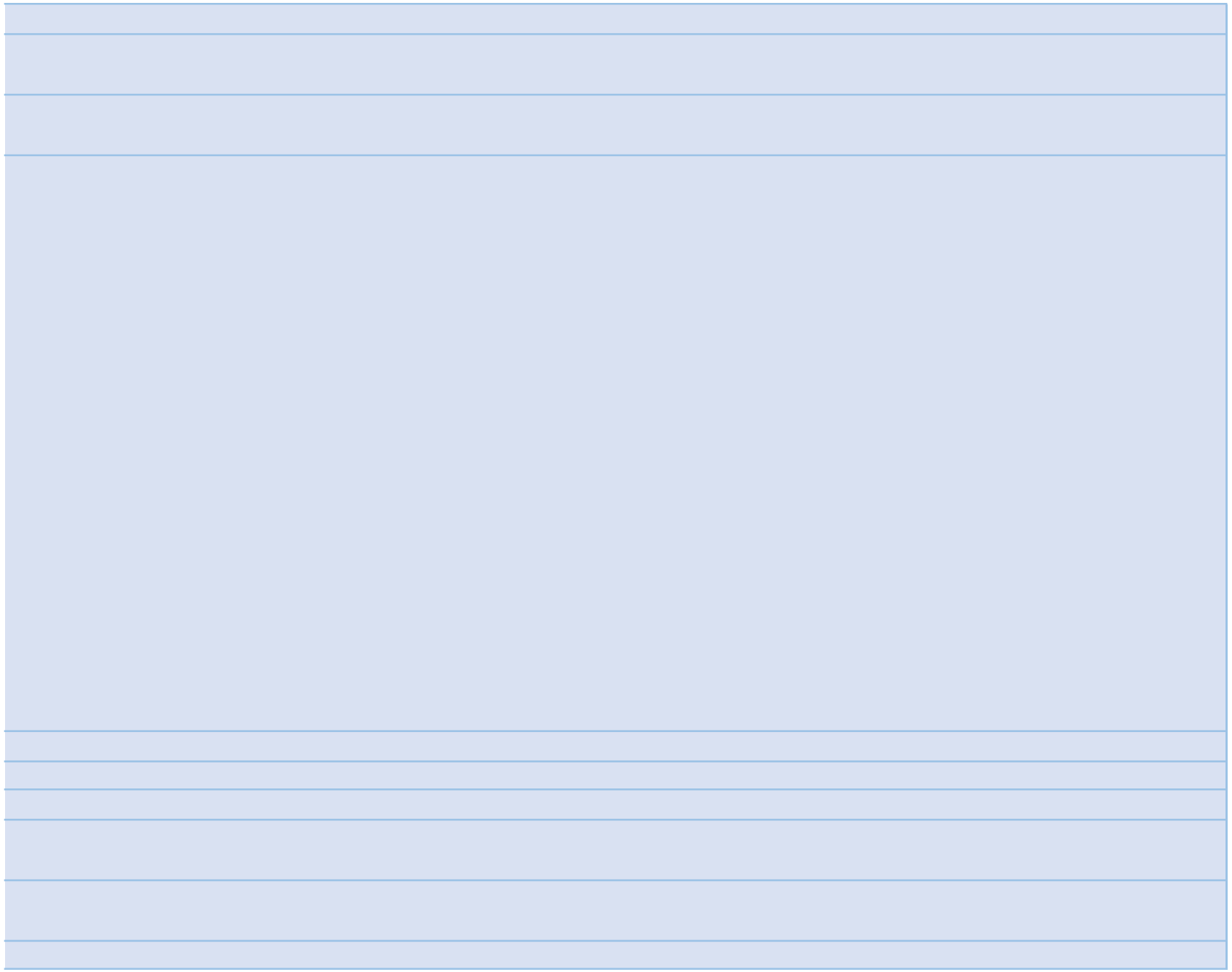
e and offline.

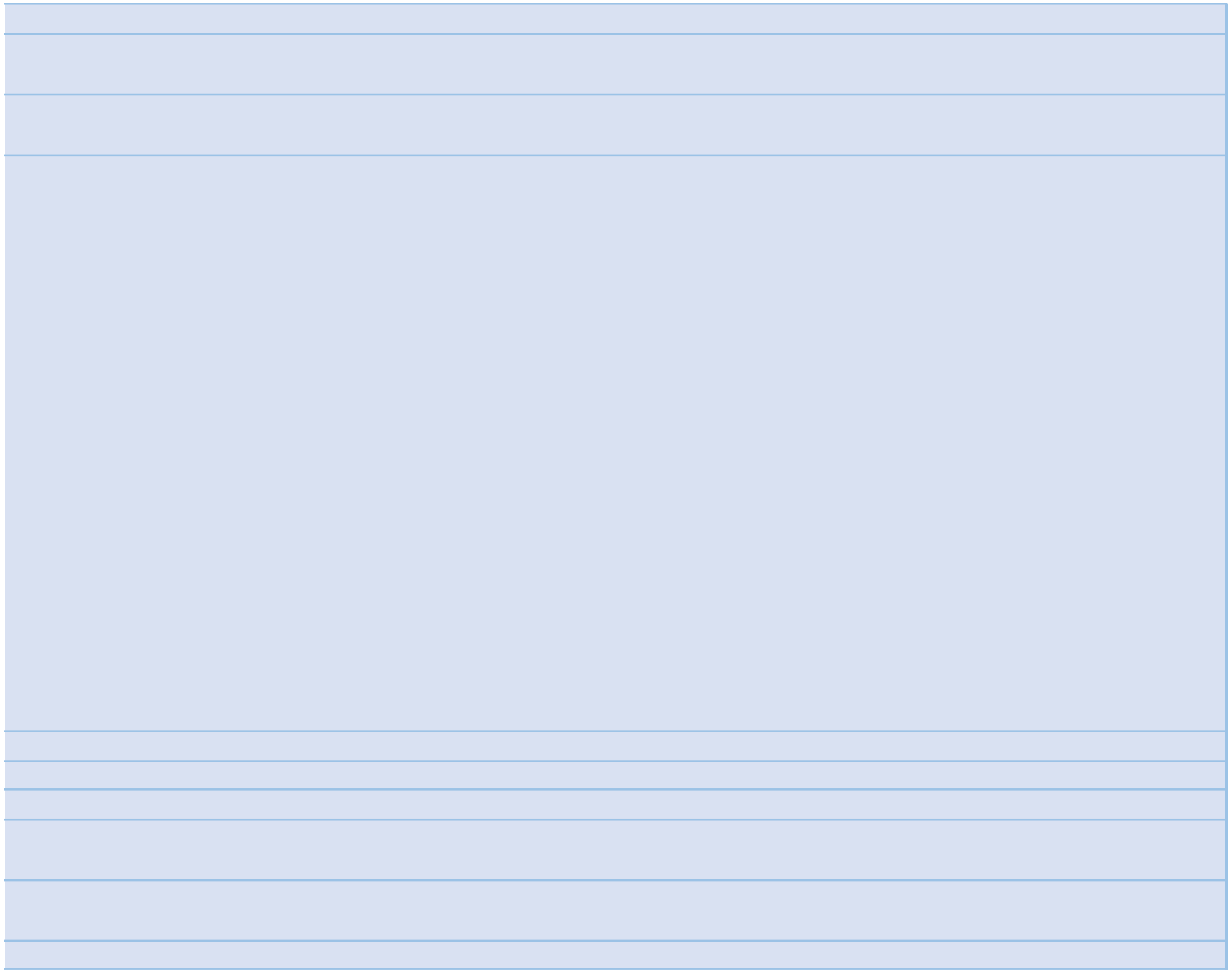
xperiences throughout your career. Each course is designed with input from leading industry experts and based on proven learning
dies, quizzes, etc. Learn at your own pace on your own time and earn valuable Continuing Professionals Education (CPE) credits tow
above and clicking the ‘My Courses’ menu item.
ase note, we do not offer time extensions for you to complete this training course.
time of purchase.Please see course description for pricing and CPEs.

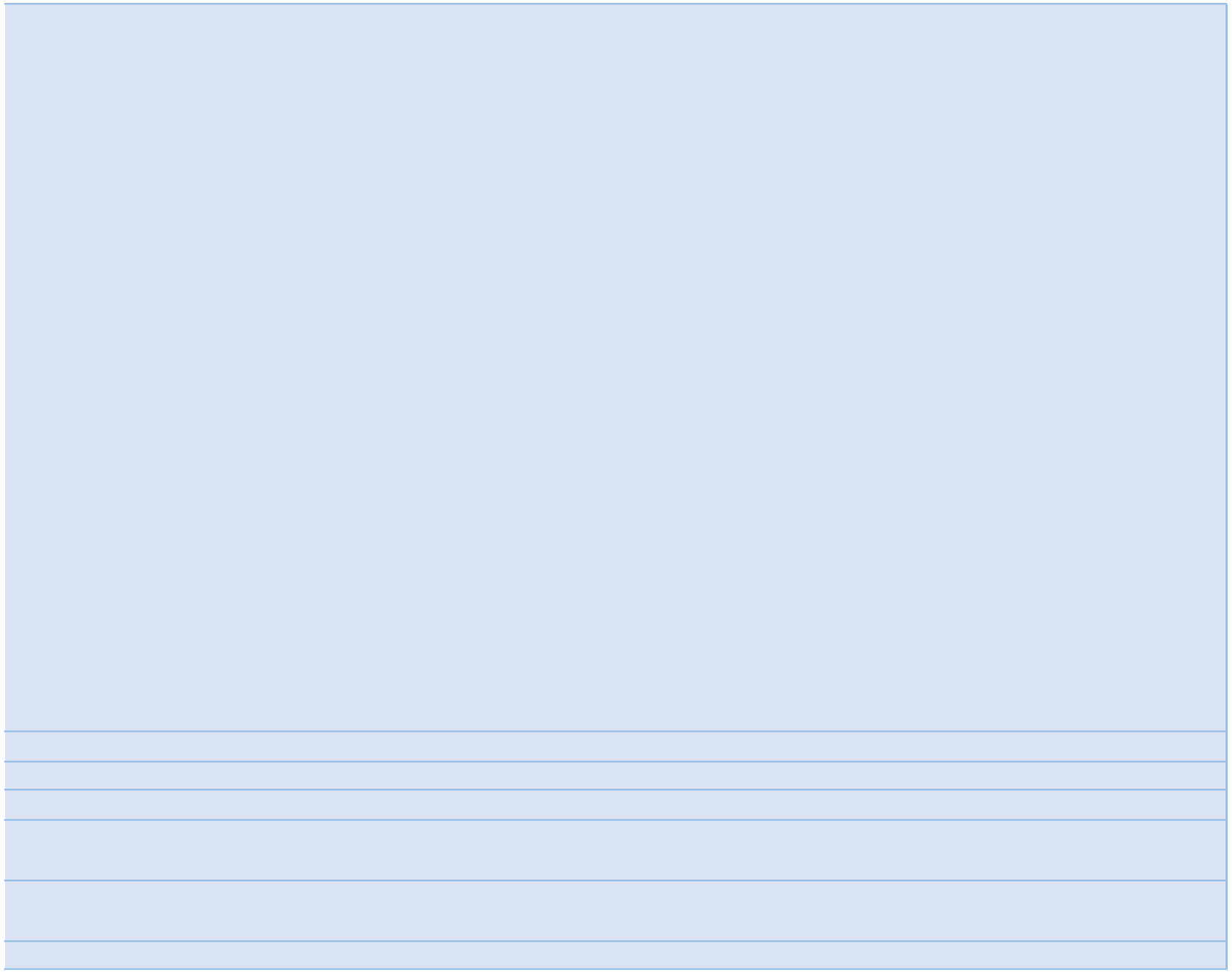


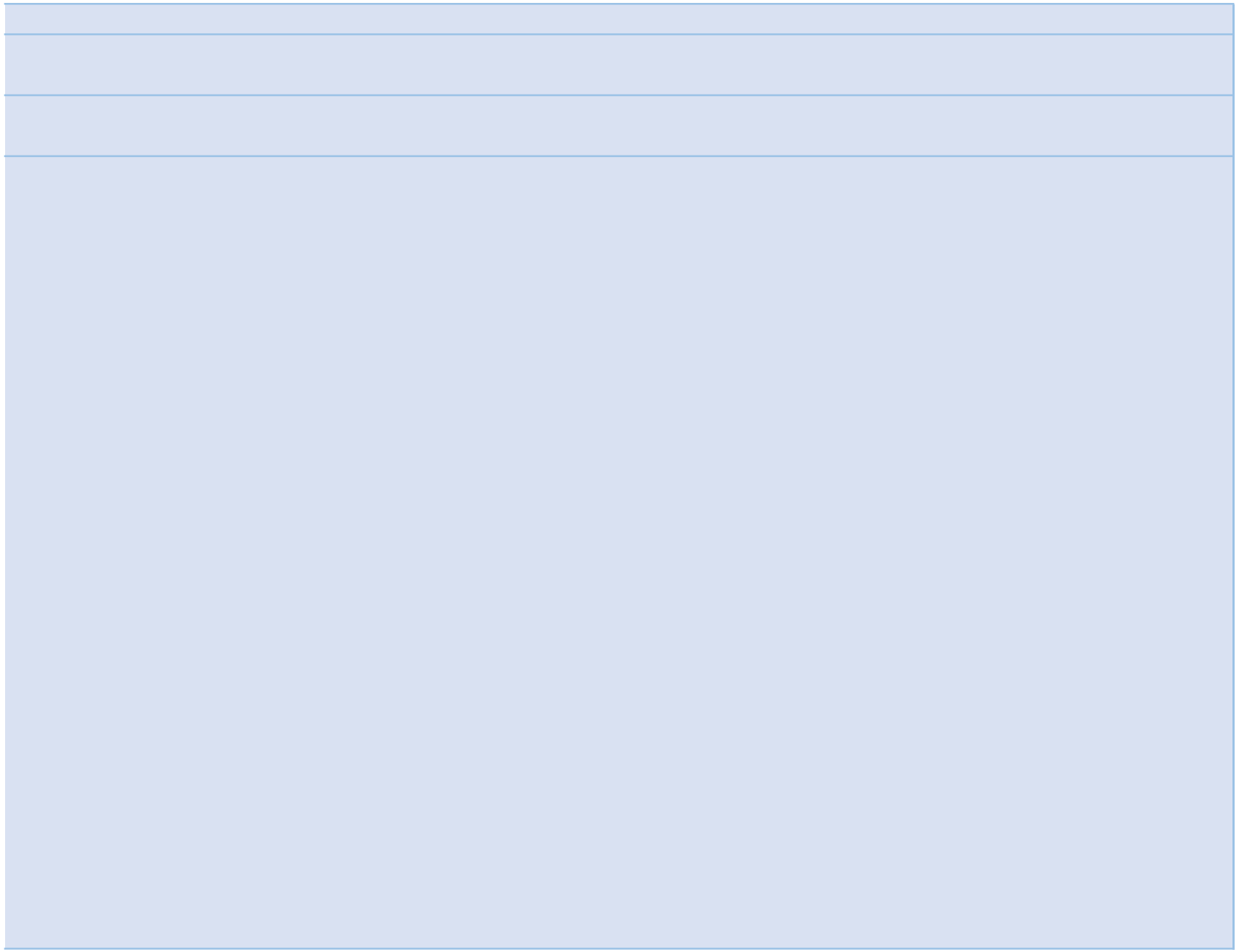


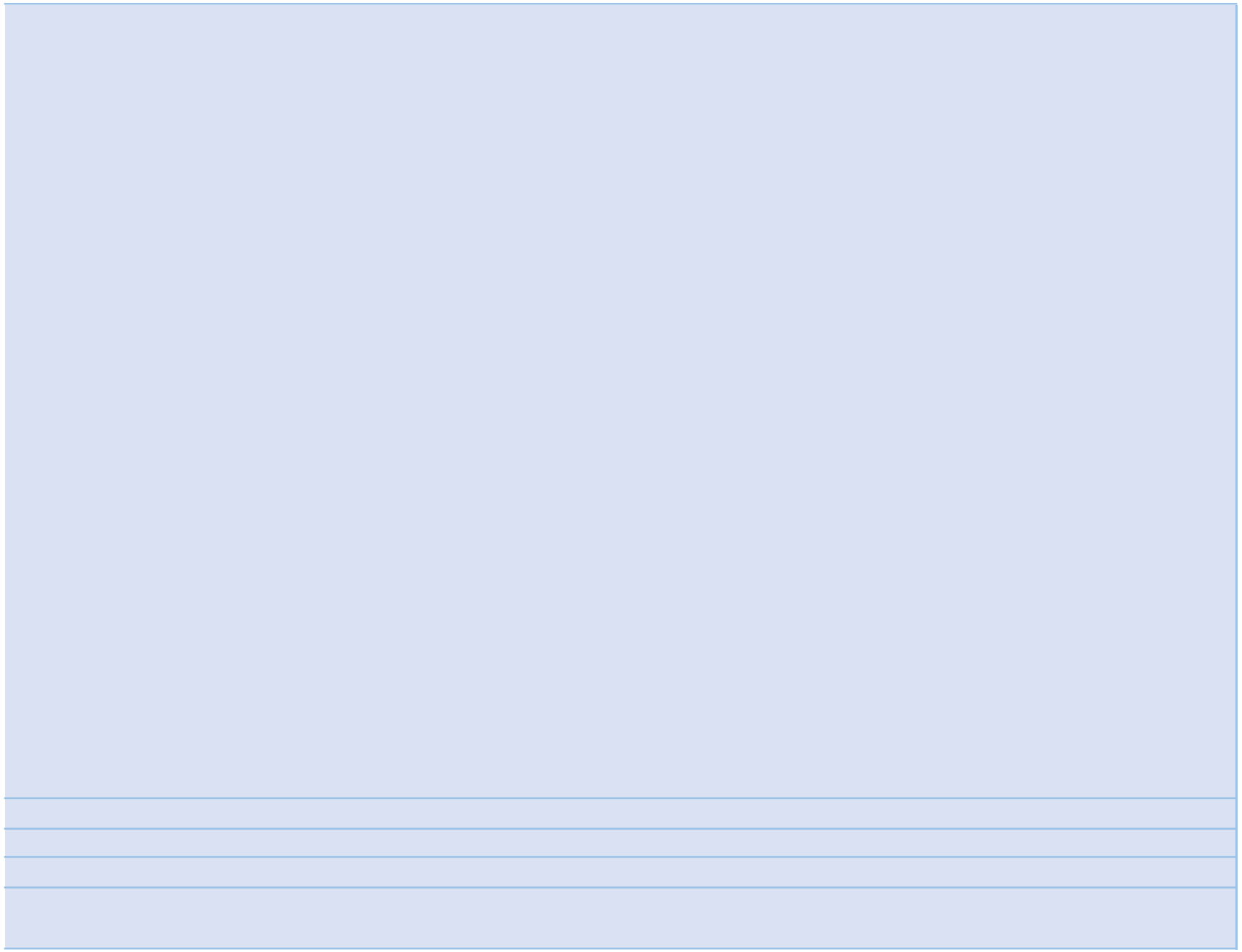


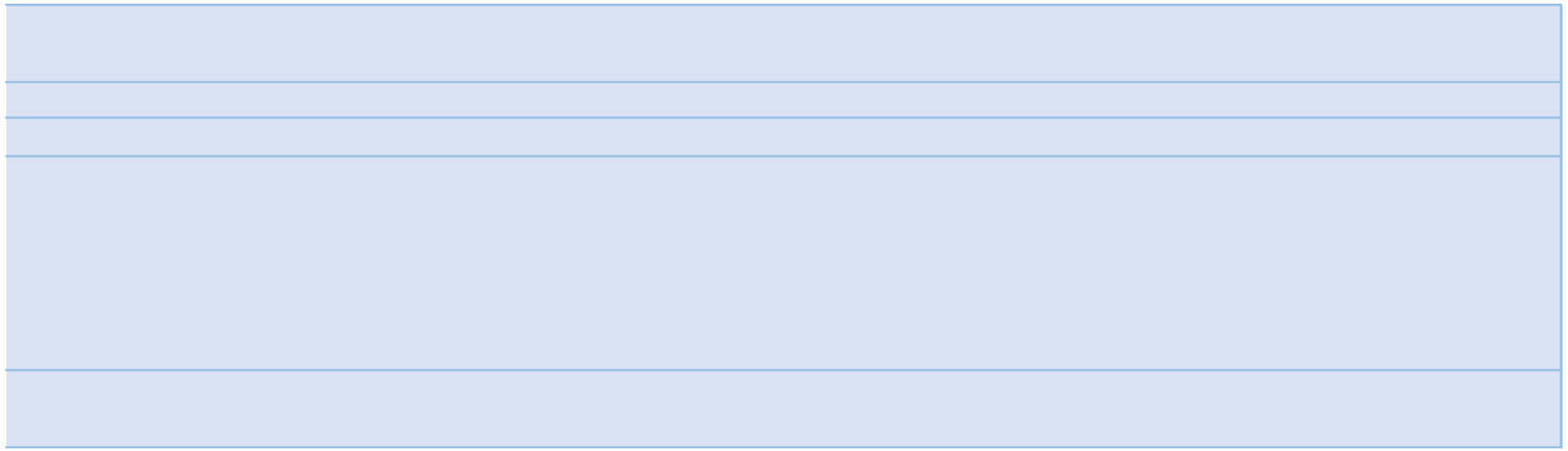


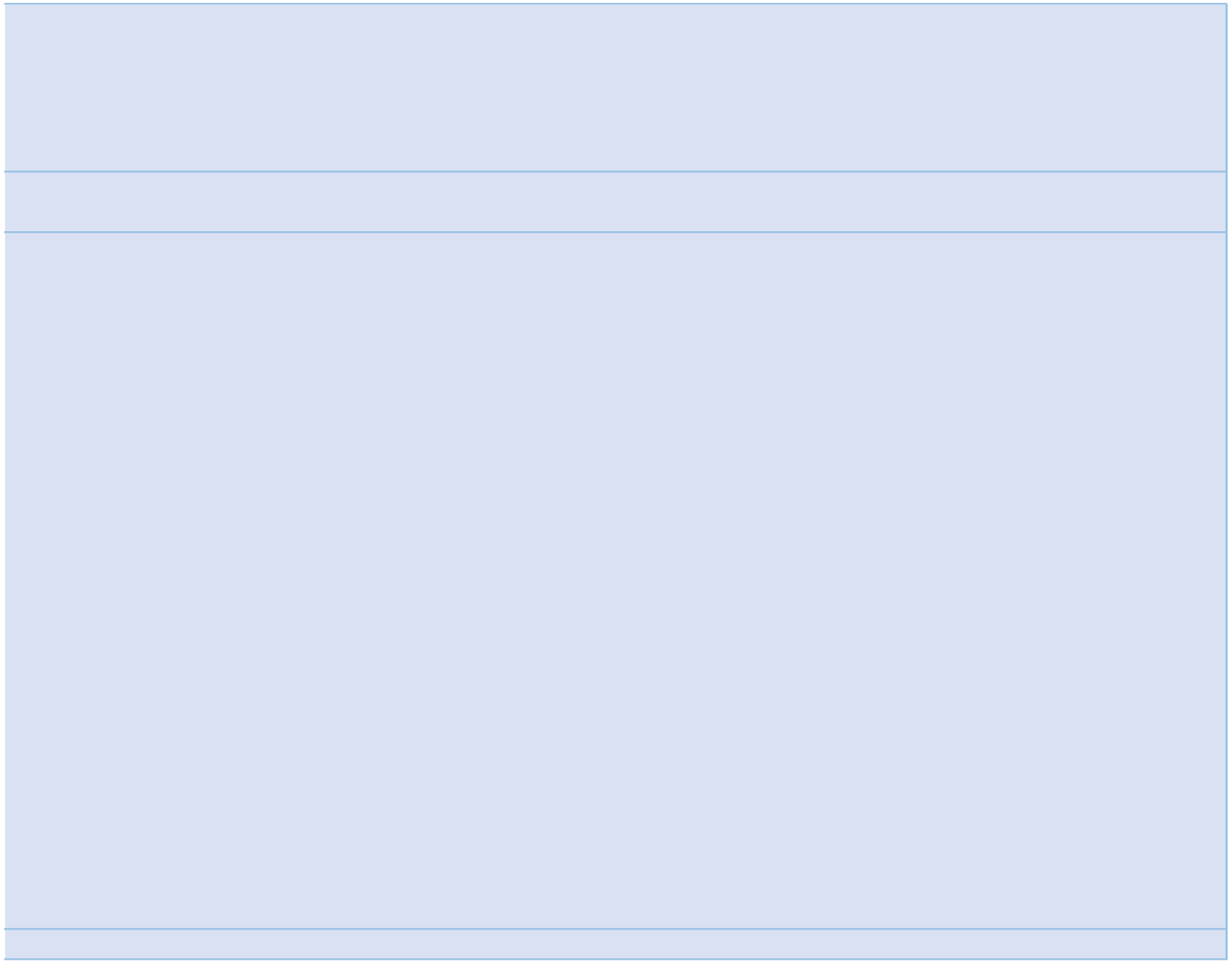


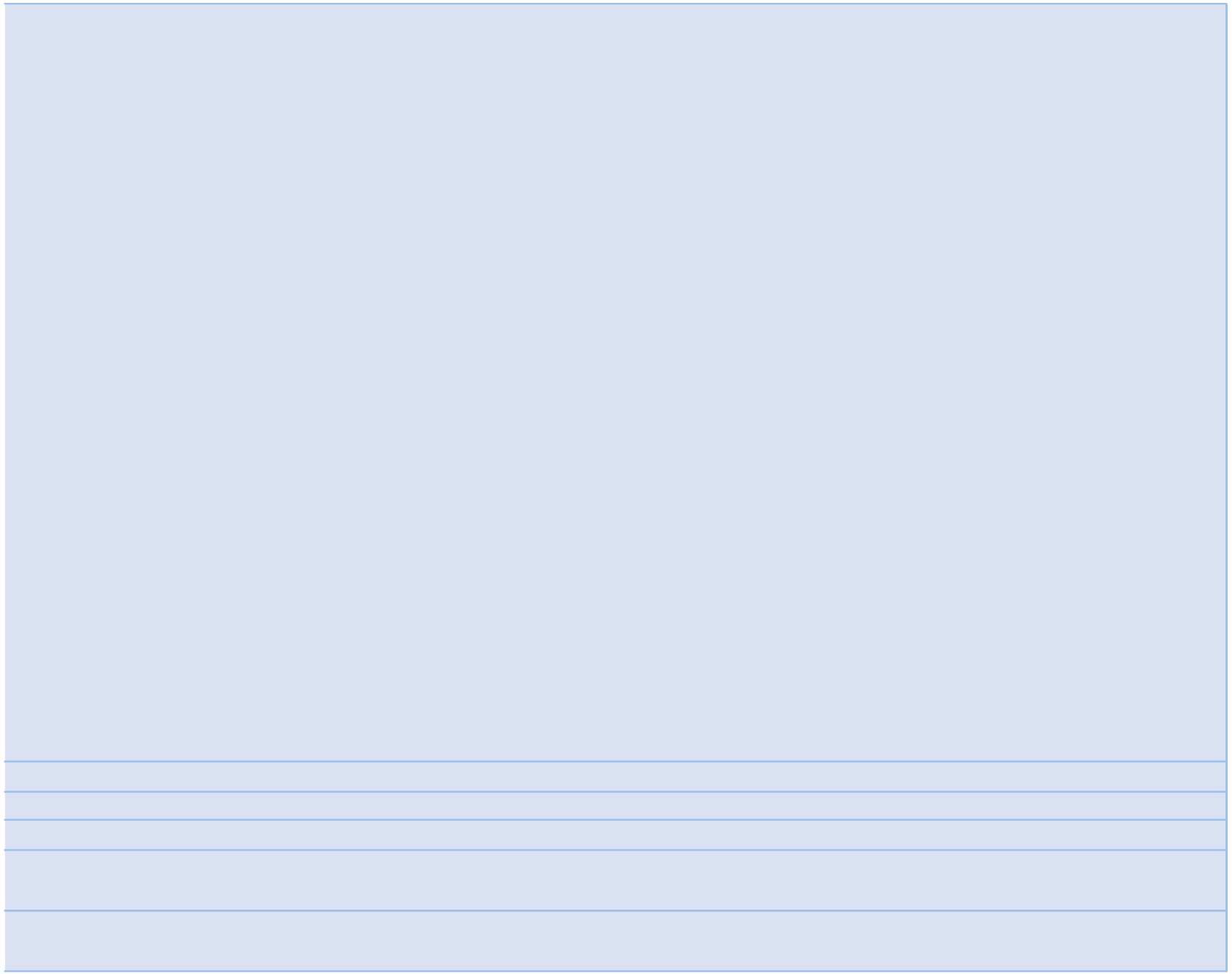


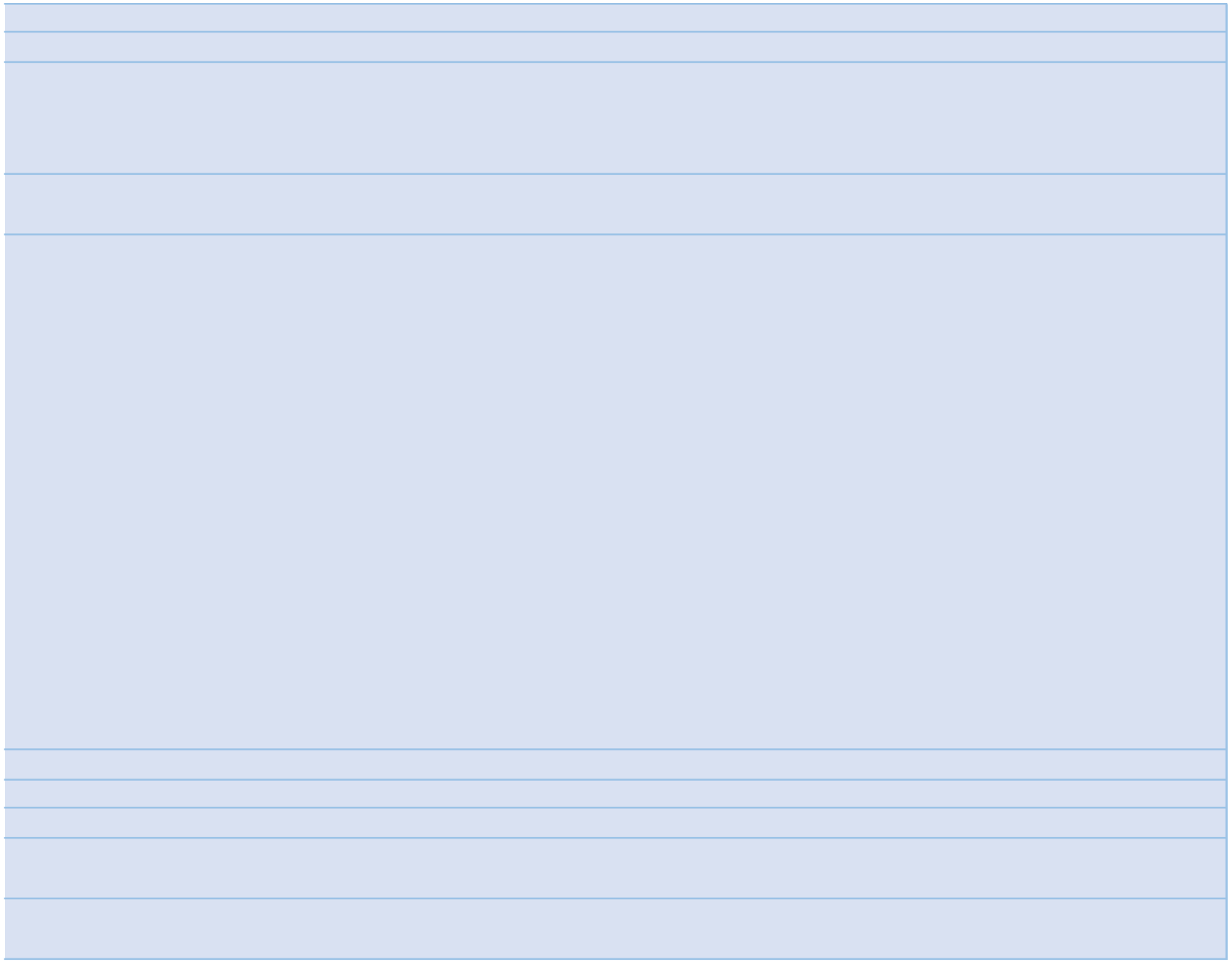


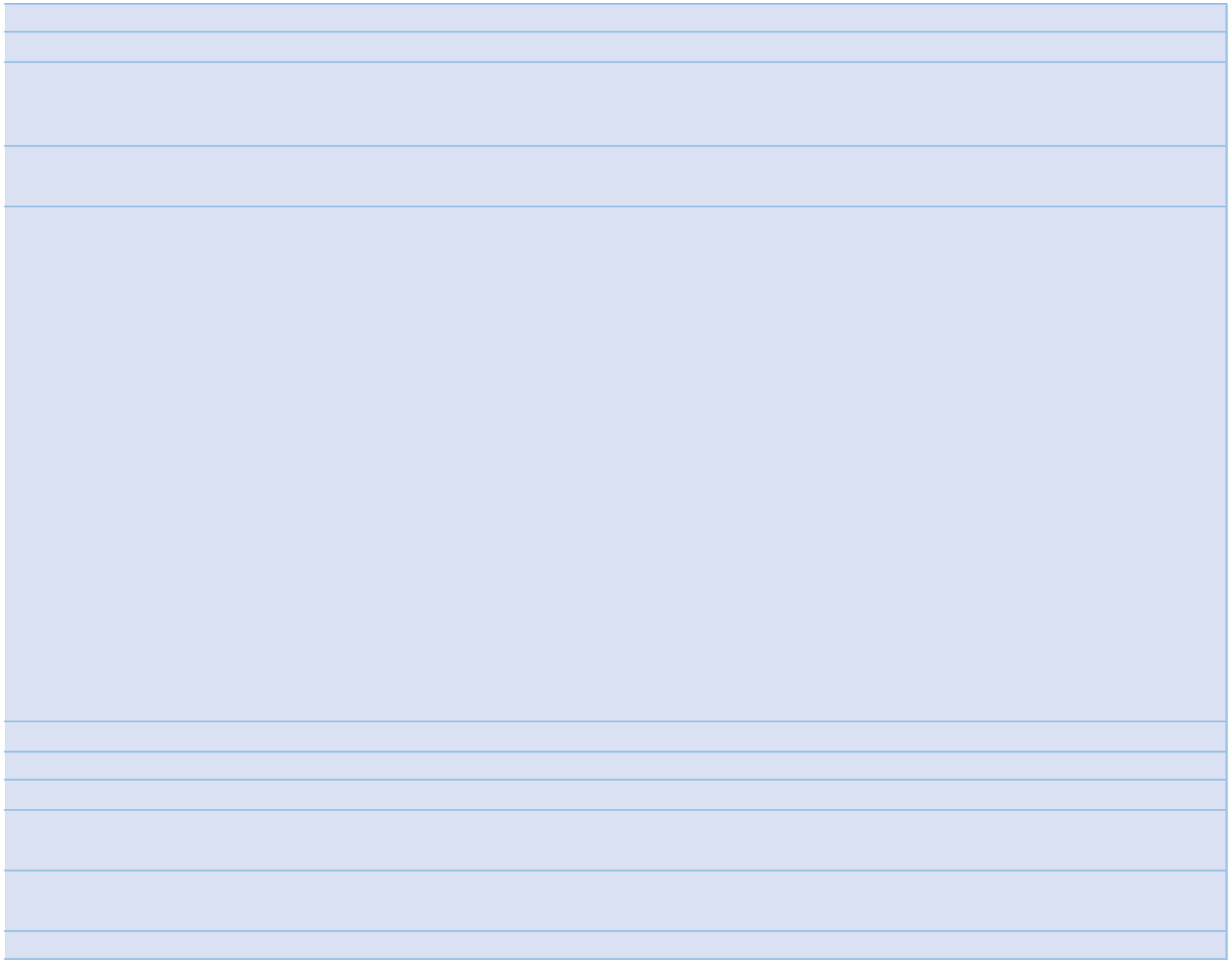


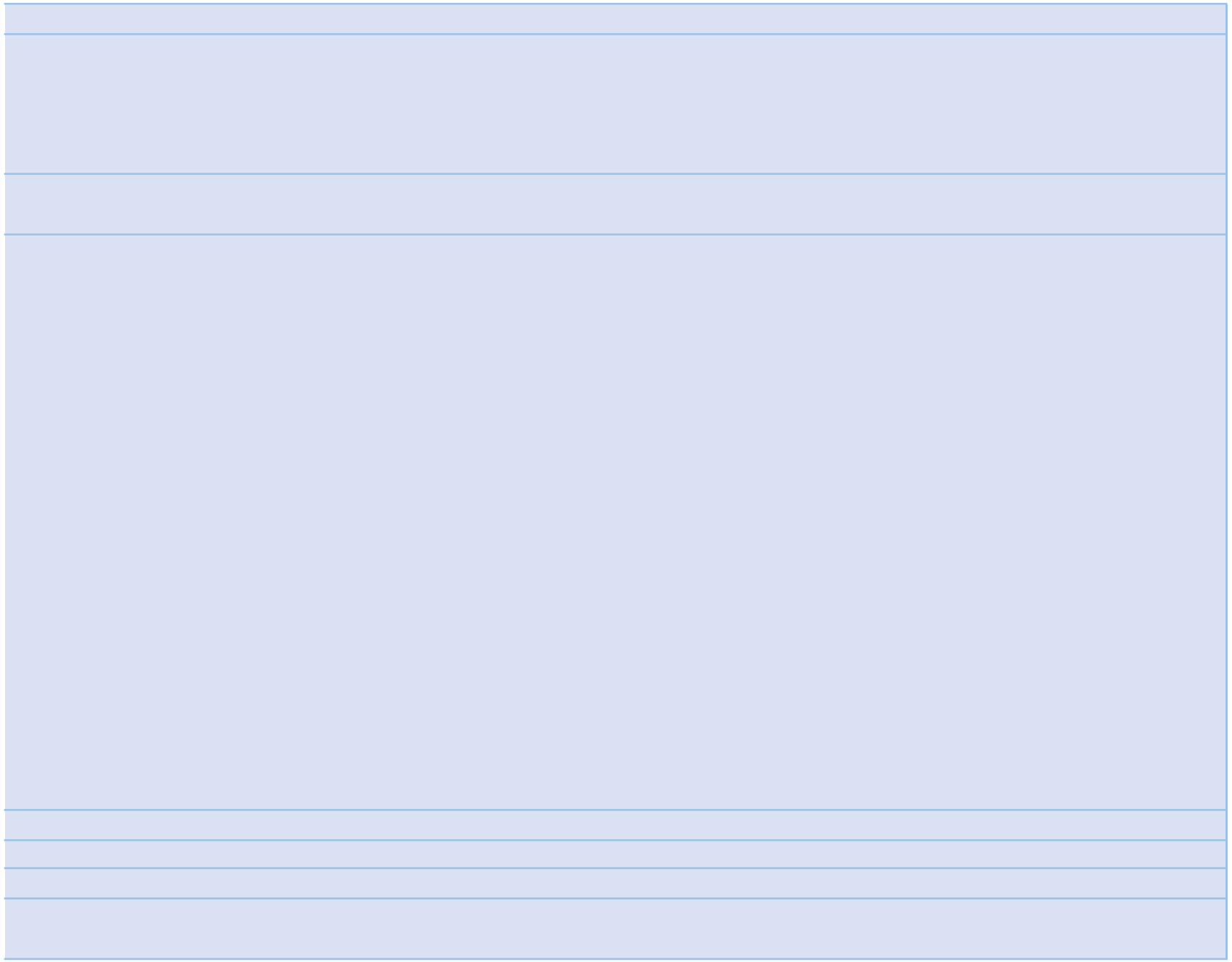


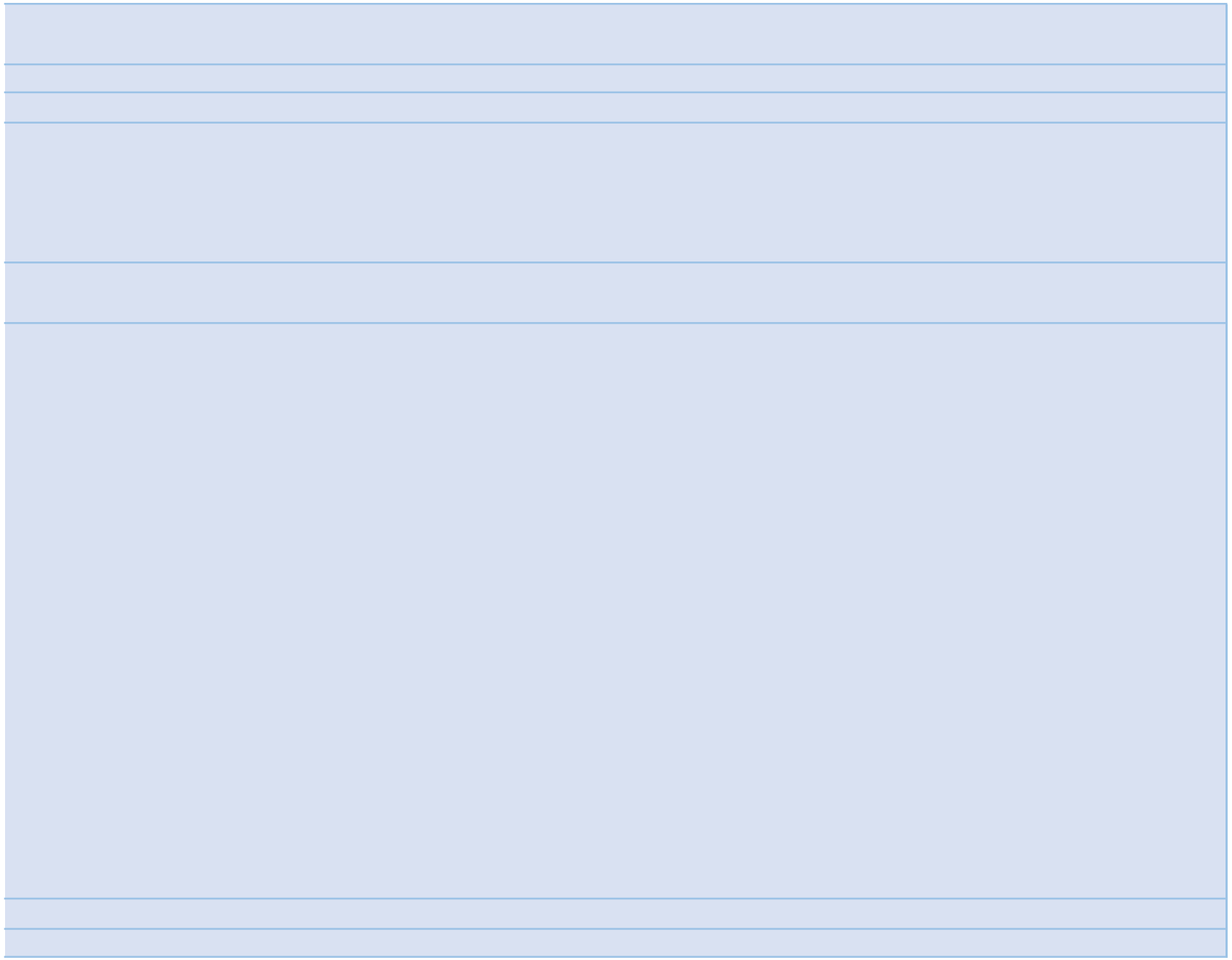


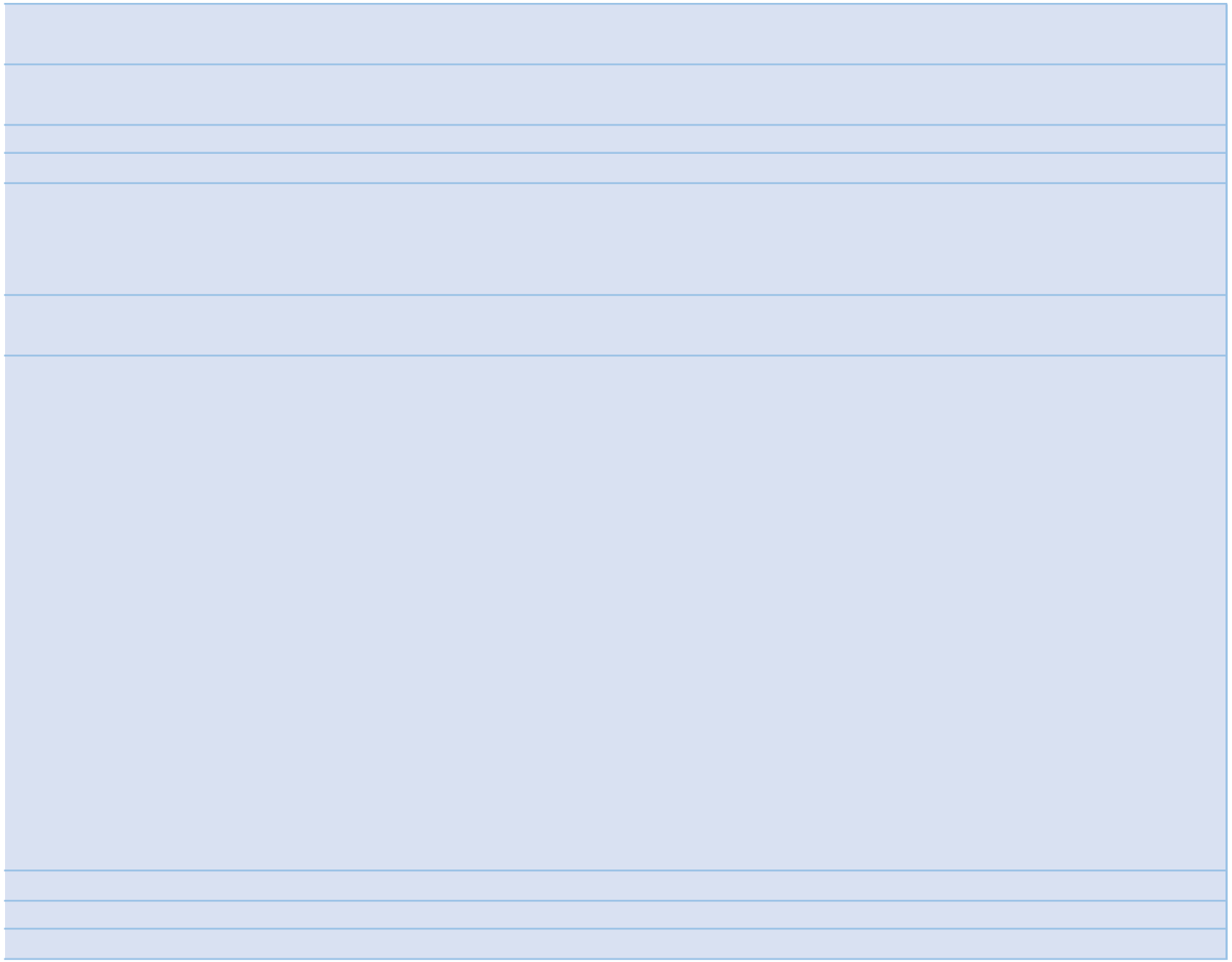


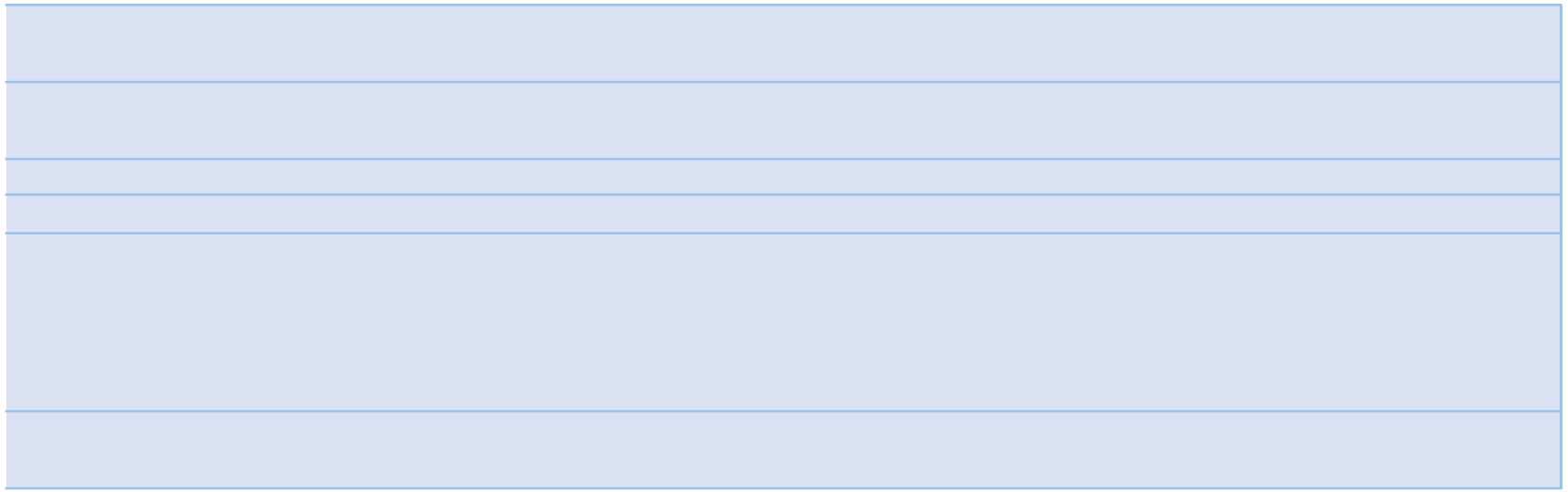


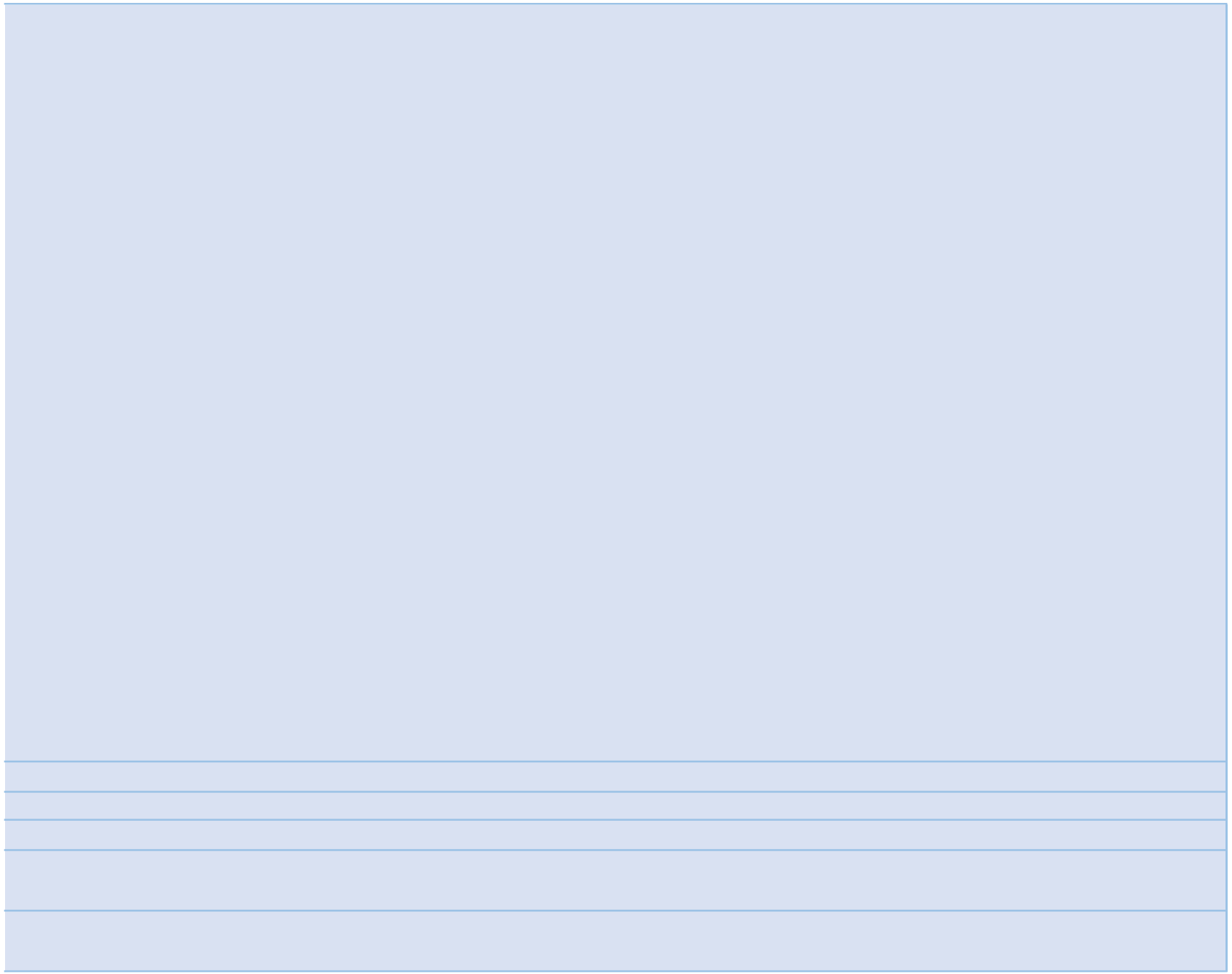


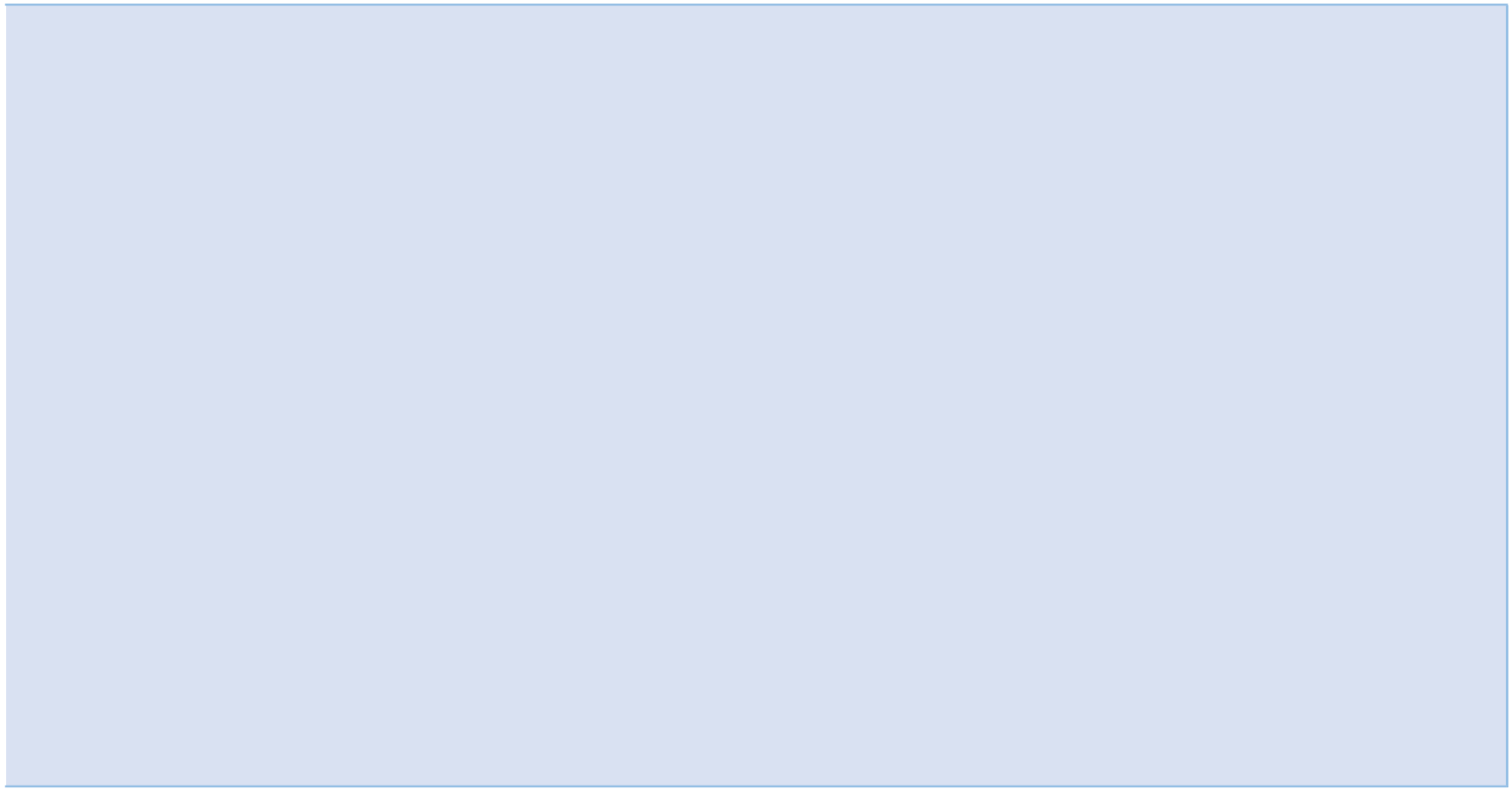


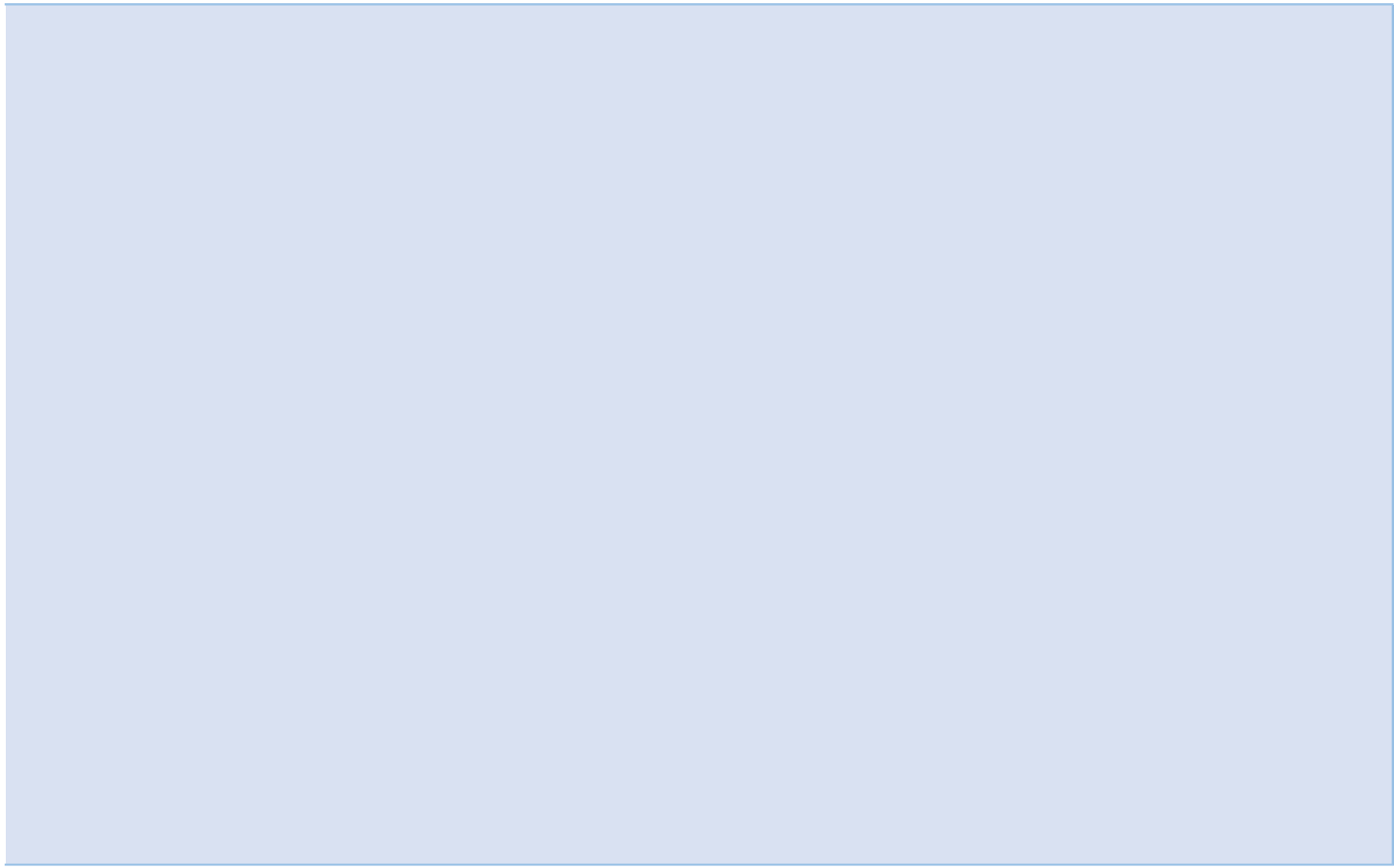


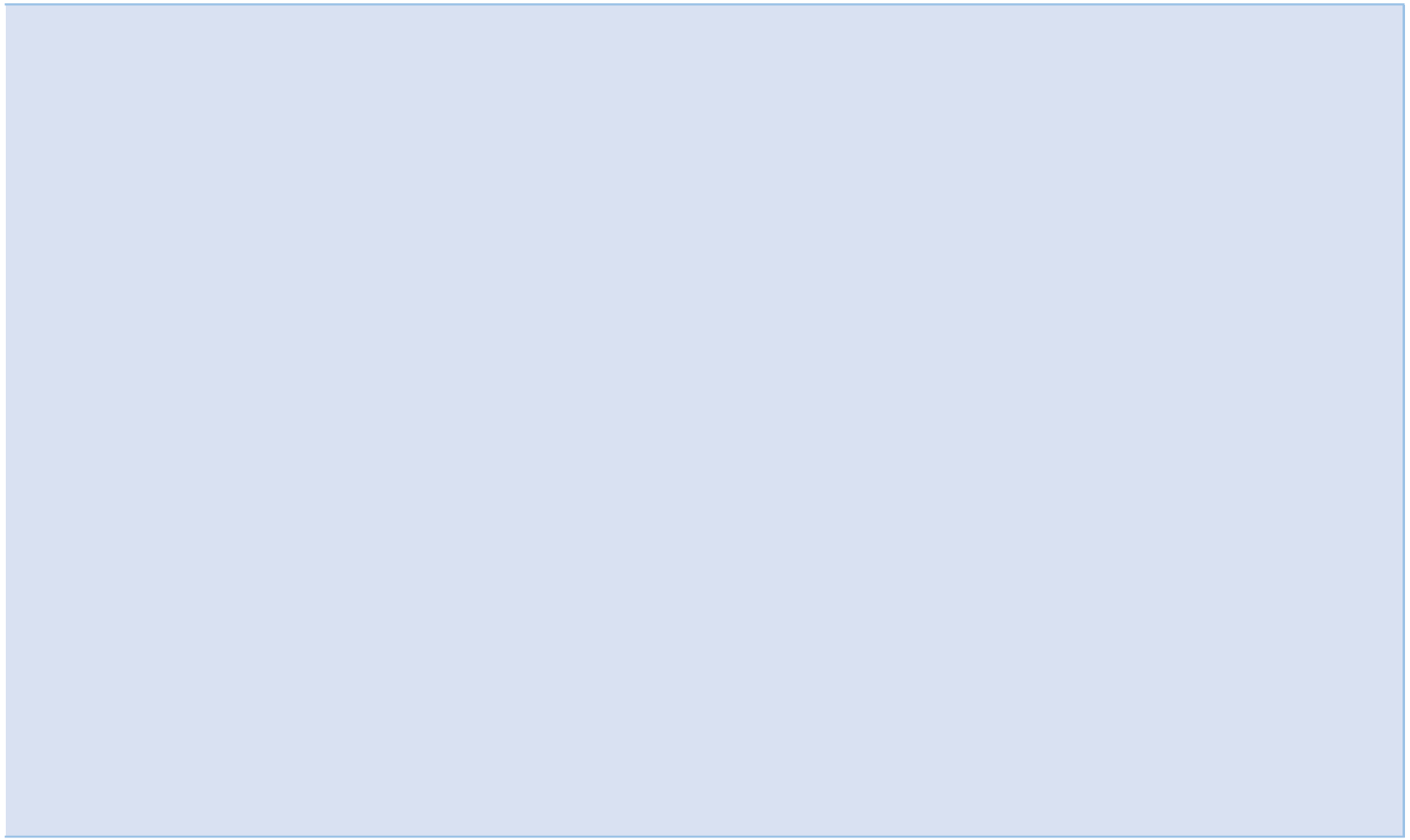


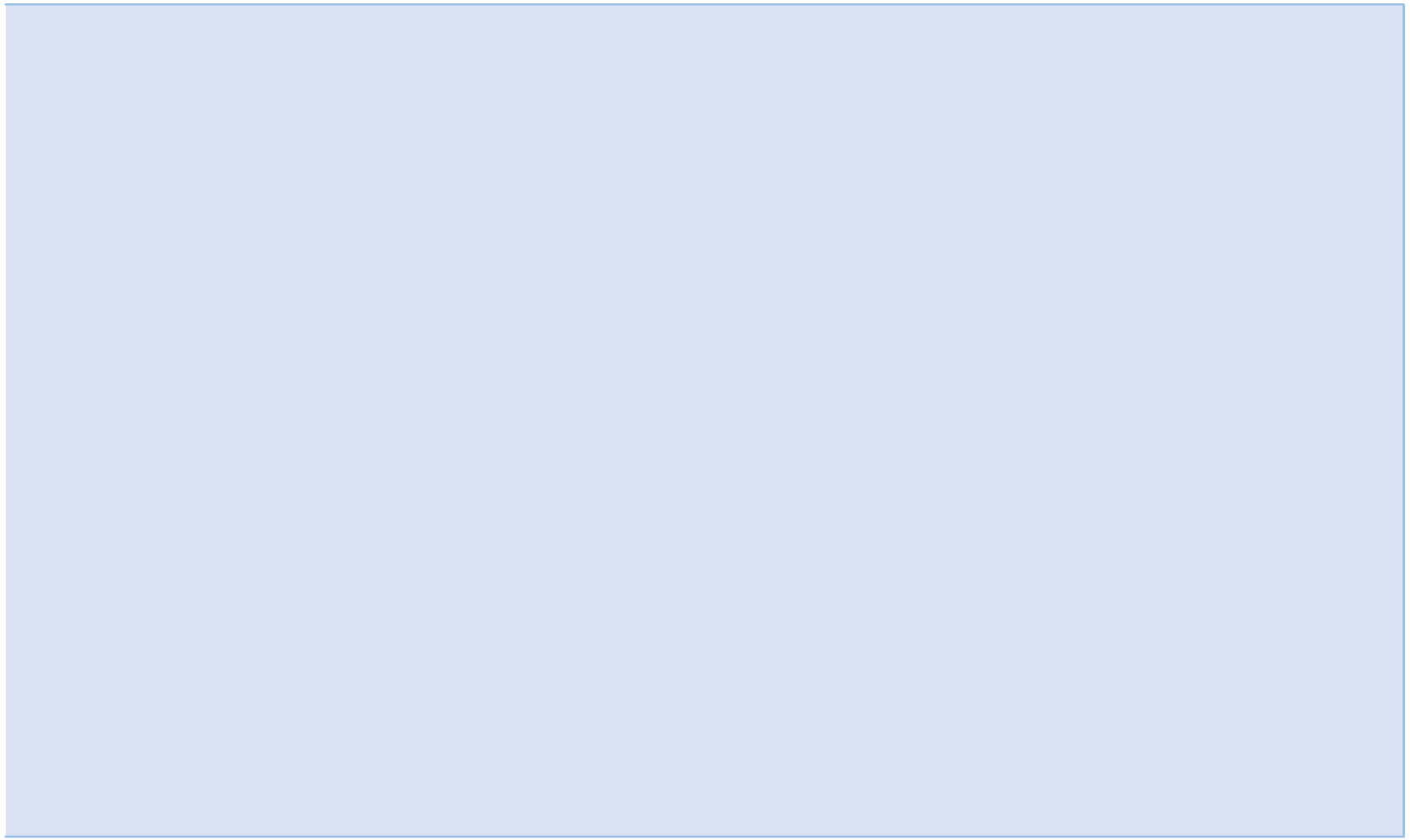


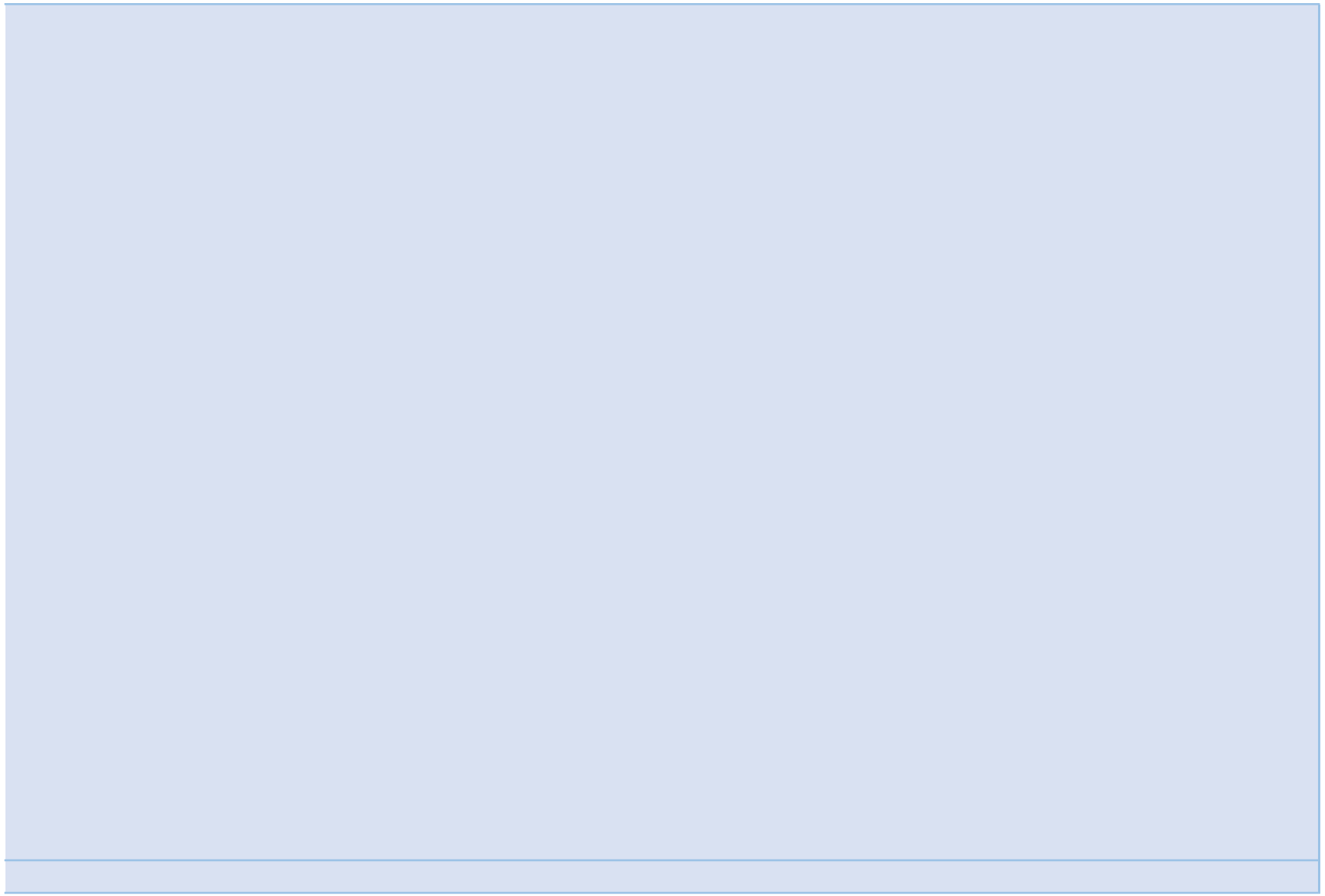


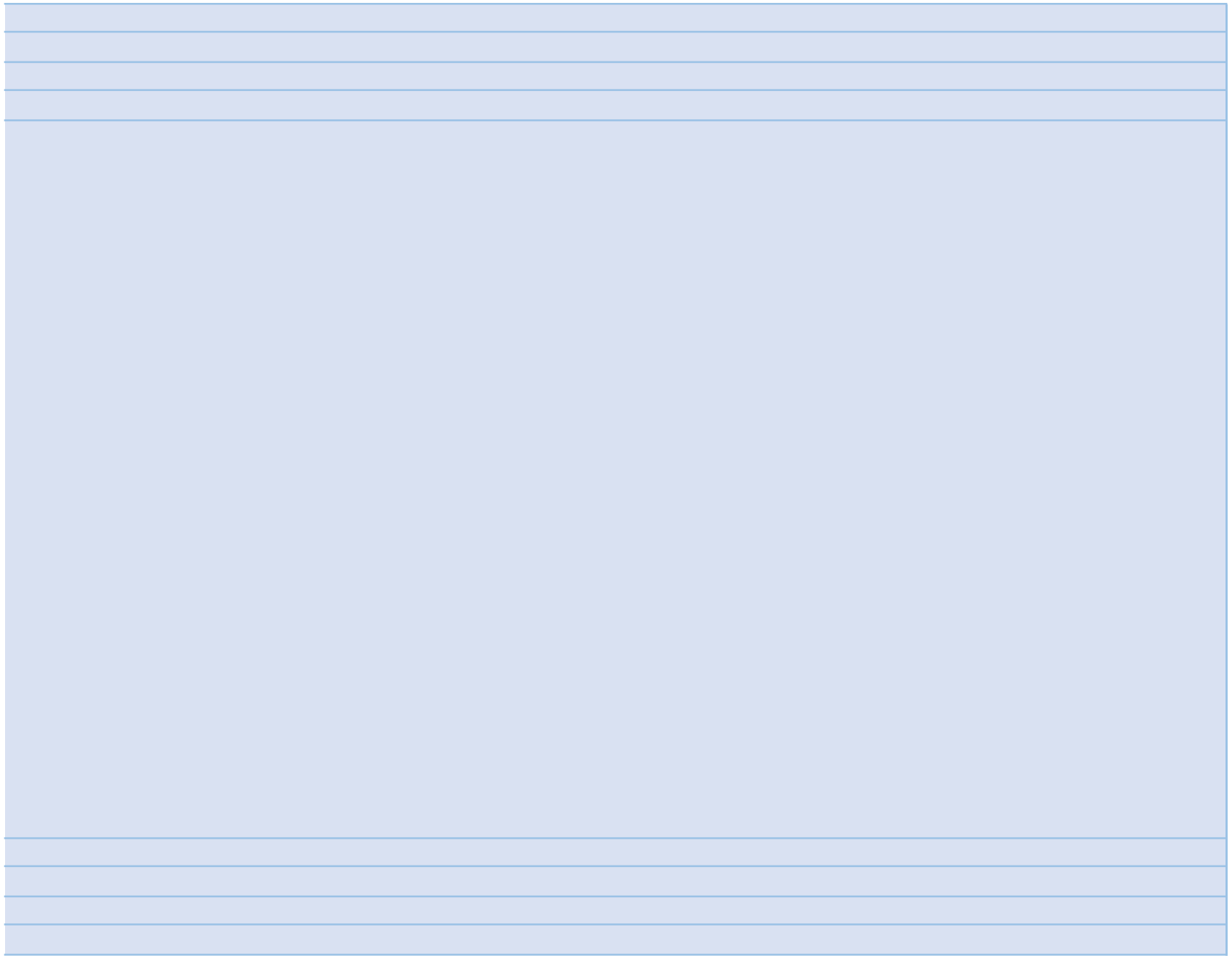












l, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and

nes in the field of information security. Successful candidates are competent in the following domains:

A one year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity pro

he SSCP examination. The Associate of ISC2 will then have two years to earn the one year required experience. You can learn more about SSC

: Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are en

reness communications)

personal device restrictions)

n Vulnerability Scoring System (CVSS), socialization, MITRE/ATT&CK model)

rnational Organization for Standardization (ISO))

is management)

wntime (MTD))

ion (PHI))
al Organization for Standardization (ISO))
ils)
SA)
on of PII data)
revocation, escrow)
, automation)

stem (DNS) cache poisoning)
nd prevention systems (IDPS))
.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+))
ucture)
, firewall zones, micro-segmentation)
EAP), Wi-Fi Protected Access 2 (WPA2), Wi-Fi Protected Access 3 (WPA3))
management)
p/code/operatin3 system (OS)/mobile code vulnerabilities)
xploits, web-based attacks, advanced persistent threat (APT))
s prevention (DLP))

e Device Management (MDM))

s))

ation technology (IT))

uditing)

he CBK and identifying areas of study that may need additional attention.

rehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

written permission. ISC2, CISSP, SSCP, CCSP, CGRC, CSSLP, HCISPP, ISSAP, ISSEP, ISSMP, CC, and CBK are registered marks of ISC2, Ir

owing is **required**:

ave your name (exactly as it appears in your exam registration) and signature, and one of the two must have your photo. For more informatio

nformation that may be used to verify the identity of a person)

these items in the test room.

e is limited, please plan appropriately. Pearson VUE test centers do not assume responsibility for your personal belongings.

ing station.

nt to review the agreement now so that you are familiar with it when you sit for your exam.

your exam and retain that information, to the extent permitted by law. Your palm vein scan will be used for the purposes of identification ver

$50 fee for exam appointment rescheduled.

tment

your appointment

in a no-show, and you will**forfeit your exam fee**. If you used the ISC2 Candidate promo code, as part of the One Million Certified in

will result in a no-show and forfeiture of all exam and rescheduling fees.

0 fee for exam appointment cancelations.

nt

ent.

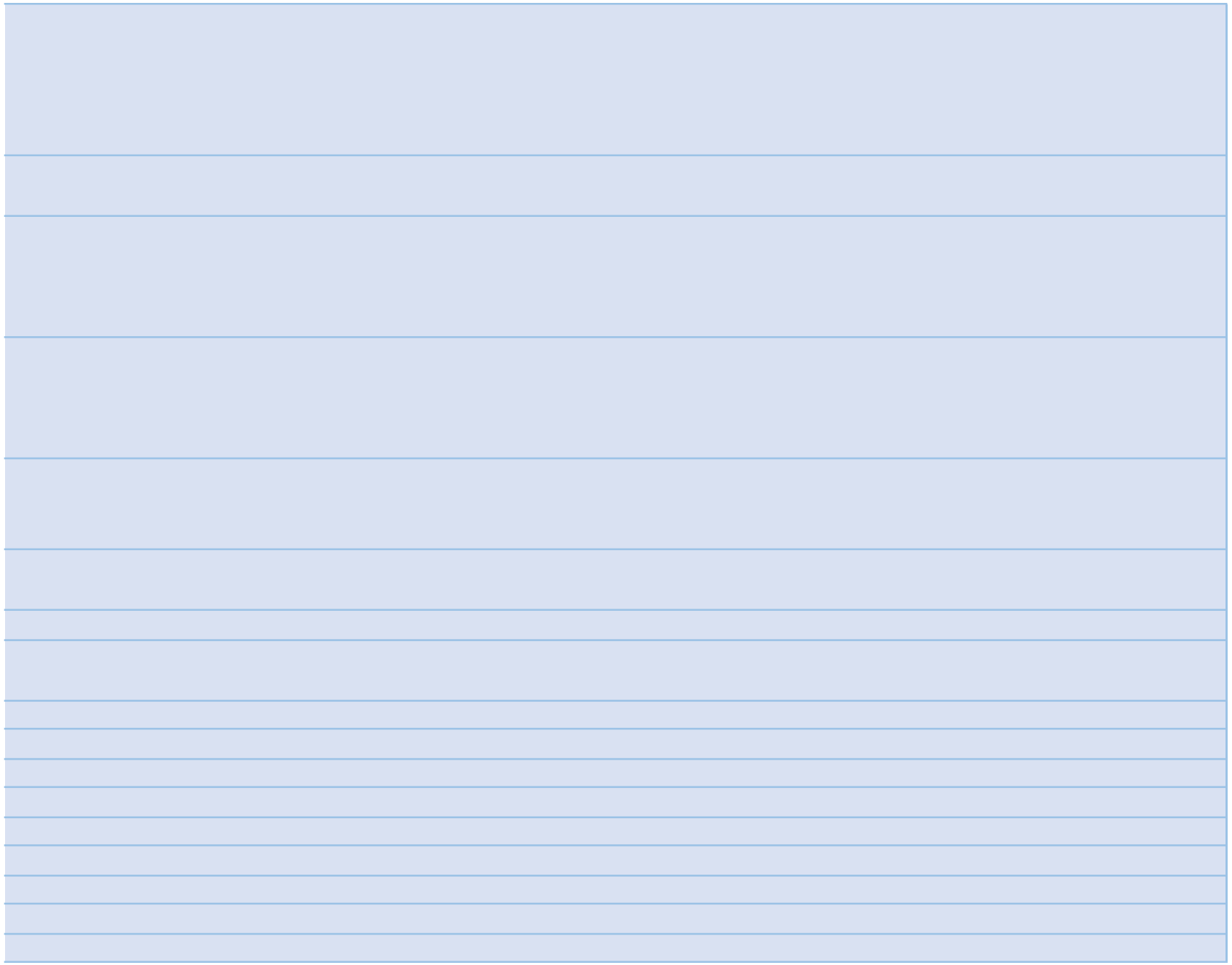
no-show, and will**forfeit your exam fee**. If you used the ISC2 Candidate promo code, as part of the One Million Certified in Cybersec

.org/uploadedFiles/Certification_Programs/CBT-Examination-Agreement.pdf. Candidates that do not agree to the terms and conditions will n

and forfeiture of exam appointment. Forfeiture of exam appointment also includes forfeiture of all exam fees. To take the examinat

ive their scores immediately upon completing their examination. In some cases, ISC2 must conduct periodic psychometric analyses
didates to skip an item, nor can items be returned to later during administration. Once an answer is confirmed it cannot be change
ently-Asked-Questions.

commodations must be requested and approved by ISC2 prior to scheduling your examination. If you wish to request an accommodation, plea



cheduled, there may be a US$50 fee to reschedule an exam with an approved accommodation.

d beyond. From PCs to data centers, our collaboration has consistently pushed technological boundaries. The strength of Lenovo’s T

ter Weekly

developers alike. Ever since its first release in 1991, Python has had a constant presence in the computer world and has become
st - ESG

am is at the forefront of innovation, building intelligent solutions that empower users across devices…

pplied Scientist to spearhead the research and development of functional autonomous agents for security scenarios....

yptography

aptive and intelligent experiences by leveraging feedback loops, analytics, and personalization techniques. We are seeking a Data Sc

d driven by curiosity, creativity, teamwork, agility, accountability and desire to learn everyday....

ineering

iven by curiosity, creativity, team work, agility, accountability and desire to learn everyday. If...

kets

is seeking a Principal Applied Scientist.The role involves building the future platform for human-robot-agent teaming. This individua

kets

is seeking a Senior Applied Scientist. The role involves building the future platform for human-robot-agent teaming. This individual

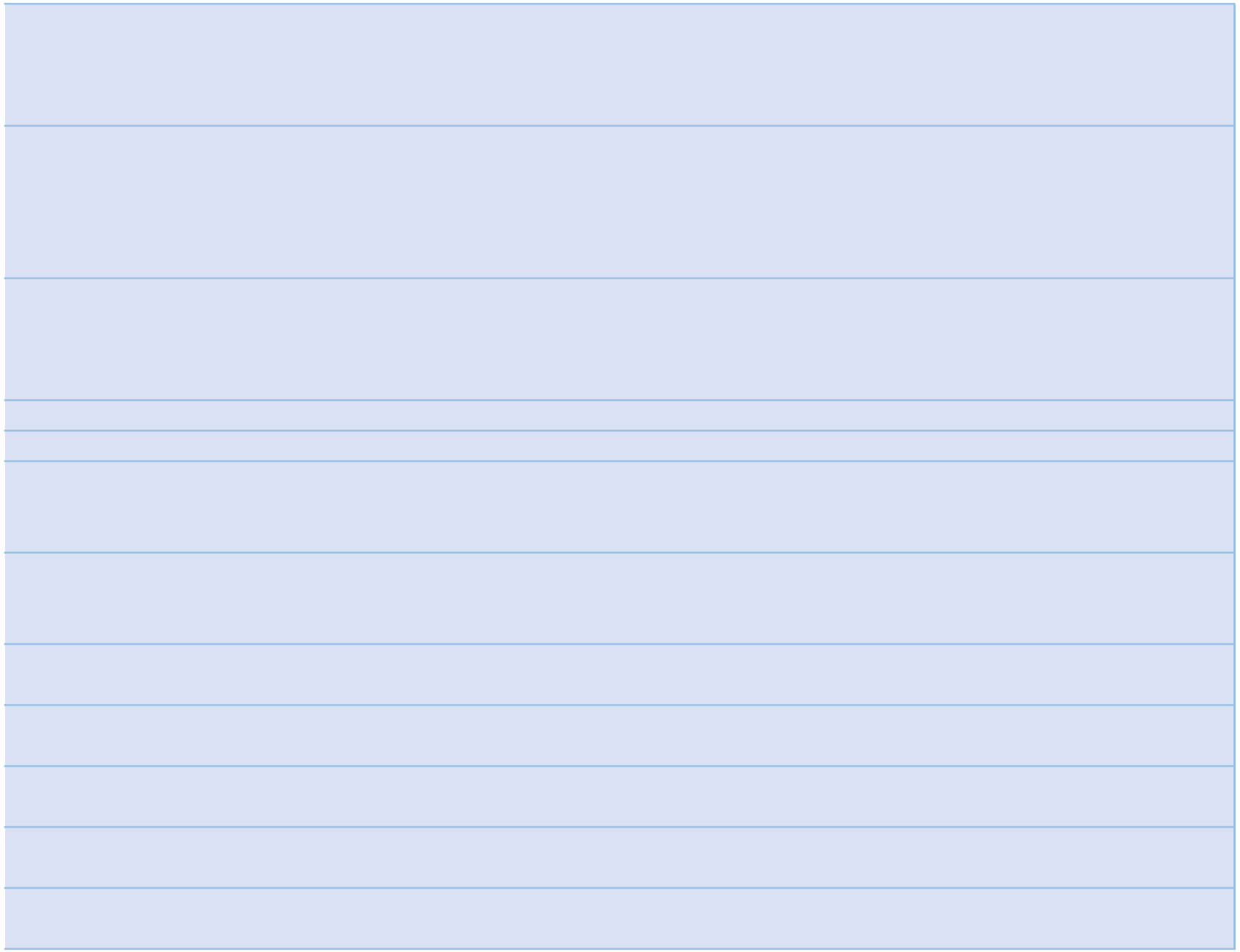
guage Models (LLMs) technologies. As a Principal Researcher, you will play a crucial role in leading,…

e, as a Senior Applied Scientist, you will collaborate with engineers, data scientists, and product managers to develop.

We are hiring a Principal Data Scientist to tackle challenges in both open-source and proprietary technologies related to

ommunications, please check your ‘junk’, ‘spam’, or ‘clutter’ folders to confirm your email settings have not redirected the emails.

ection Regulation (GDPR), then please visit Privacy Management for more information.



good cause shown.

rs.

urity service provider.

onduct and statutory mandate.

awareness.

on proper documentation, clear communication, and adherence to statutory mandates.

r)

stered trademarks of BlockMark Technologies Ltd. Registered in England with Company Number10821944. VAT Registration Numbe

MT)

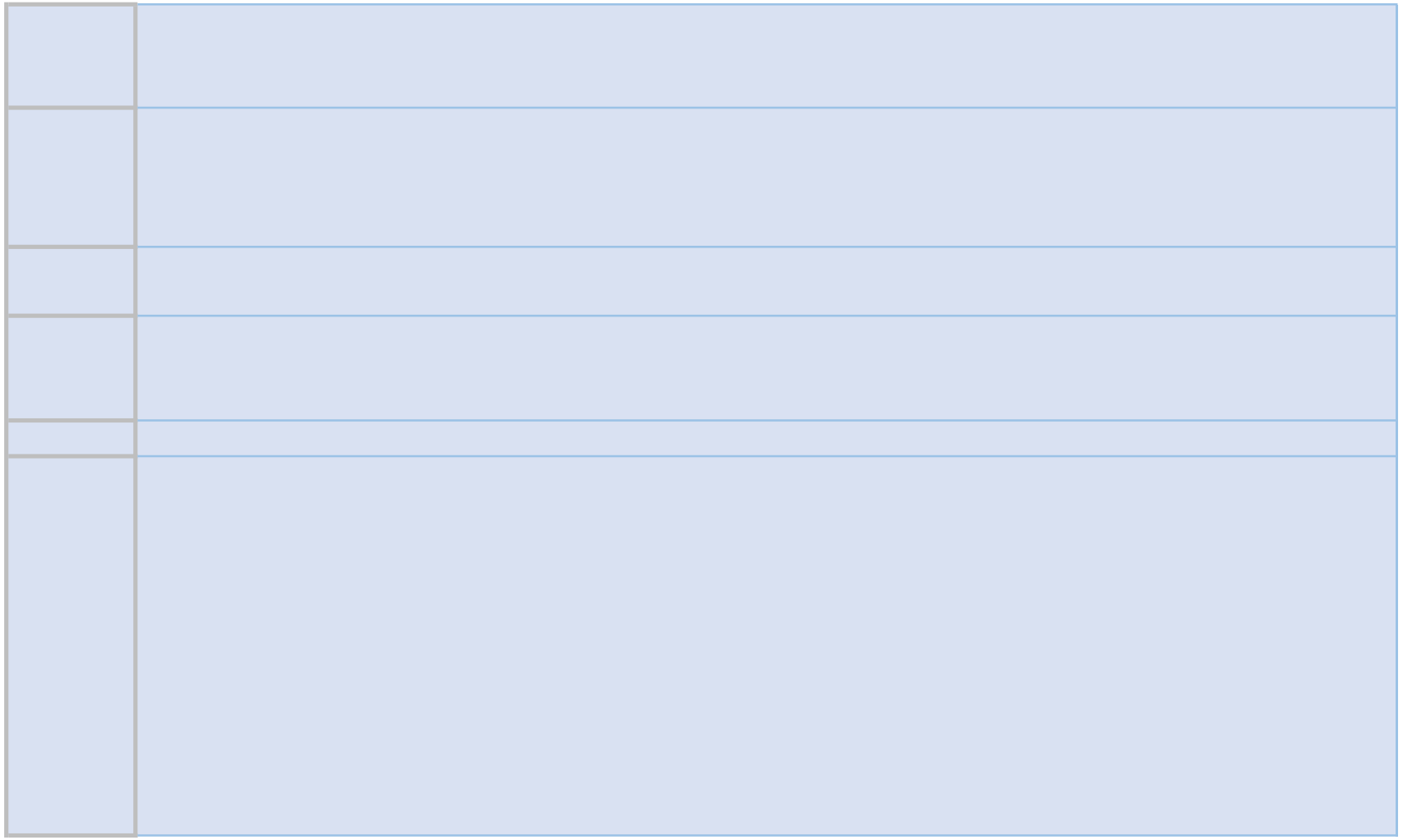
ce on Thursday 6th March 2025 - 08:05:08(GMT)

2025 - 08:49:36(GMT)

arch 2025 - 08:49:01(GMT)

March 2025 - 08:47:55(GMT)

March 2025 - 08:46:52(GMT)



March 2025 - 08:58:01(GMT)

Issued by	Issued to	Valid from	Expires	Inspected on	ID	
The IASME Consortium Ltd	THE SECURITY INSTITUTE	12/9/2024, 1:28 PM	12/9/2025, 1:28 PM	3/6/2025, 10:59 AM	f9751c2e-5511-4658-b82a-f79a190d1a8d	
	EFFECTIVE SECURITY SERVICES LIMITED T/A PROFESSIONAL SECURITY	1/30/2024, 12:31 PM	1/30/2025, 12:31 PM	3/6/2025, 10:59 AM	f2846e61-8c15-49ba-ae13-6e36c54b1440	

7/22/2024, 7:27 PM	7/22/2025, 7:27 PM	3/6/2025, 10:58 AM	193795ce-b169-4ebb-9a0e-6bfe12fbb738		

6/26/2024, 12:44 AM	6/26/2025, 12:44 AM	3/6/2025, 10:58 AM	ff88f740-06ad-4c0b-8a54-8de97b382a8a		

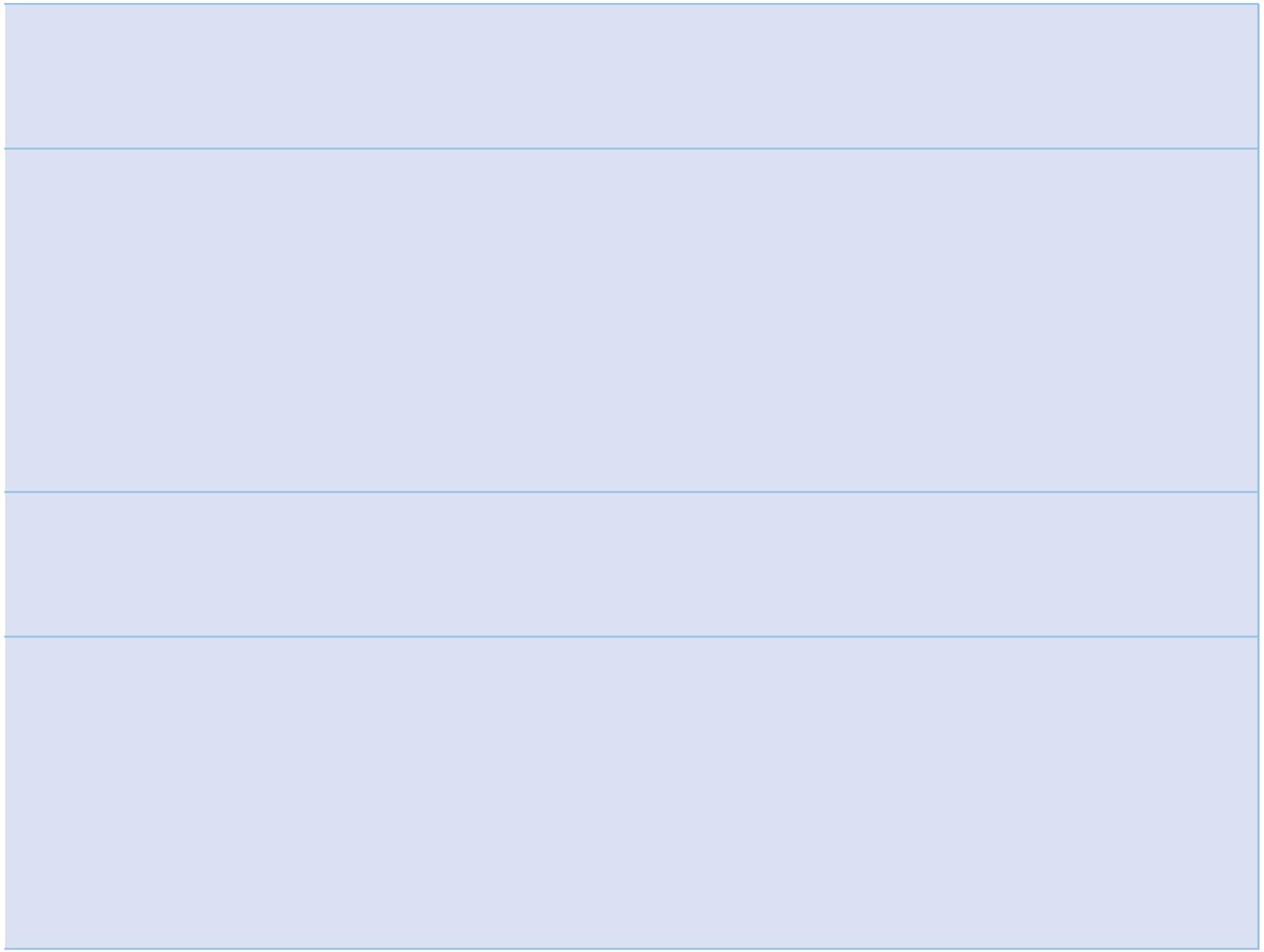
7/9/2024, 11:23 PM	7/9/2025, 11:23 PM	3/6/2025, 10:57 AM	d9307d3a-21f3-4127-bd5c-3908f42bebf4
5/15/2024, 3:35 PM	5/15/2025, 3:35 PM	3/6/2025, 10:50 AM	032c8f69-6481-4fdc-bb0a-abb5a93cfd26

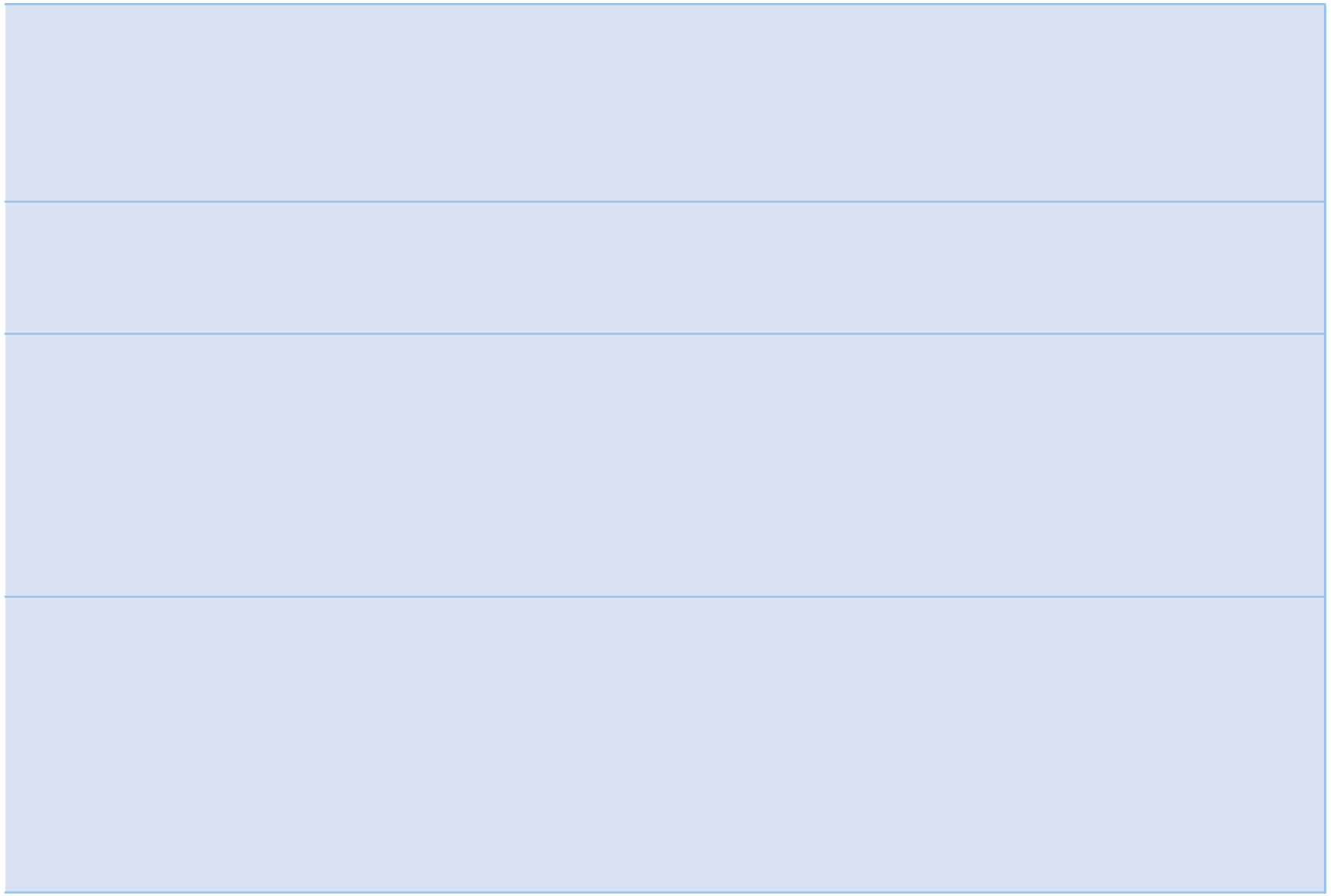
1/3/2024, 1:54 PM	1/3/2025, 1:54 PM	3/6/2025, 10:49 AM	98240e15-5f1b-4dd2-8ea0-da63276762b4
8/16/2024, 2:11 PM	8/16/2025, 2:11 PM	3/6/2025, 10:47 AM	16b1cc59-a0e5-4ab4-977b-e22e556140e2
3/2/2023, 5:25 PM	3/2/2024, 5:25 PM	3/6/2025, 10:47 AM	4e6d6d2e-ac07-441c-bc2d-db0e5a60c1ef
11/28/2024, 9:52 AM	11/28/2025, 9:52 AM	3/6/2025, 10:46 AM	ca683bd6-86ec-4e29-9fbd-3f3d1398097b

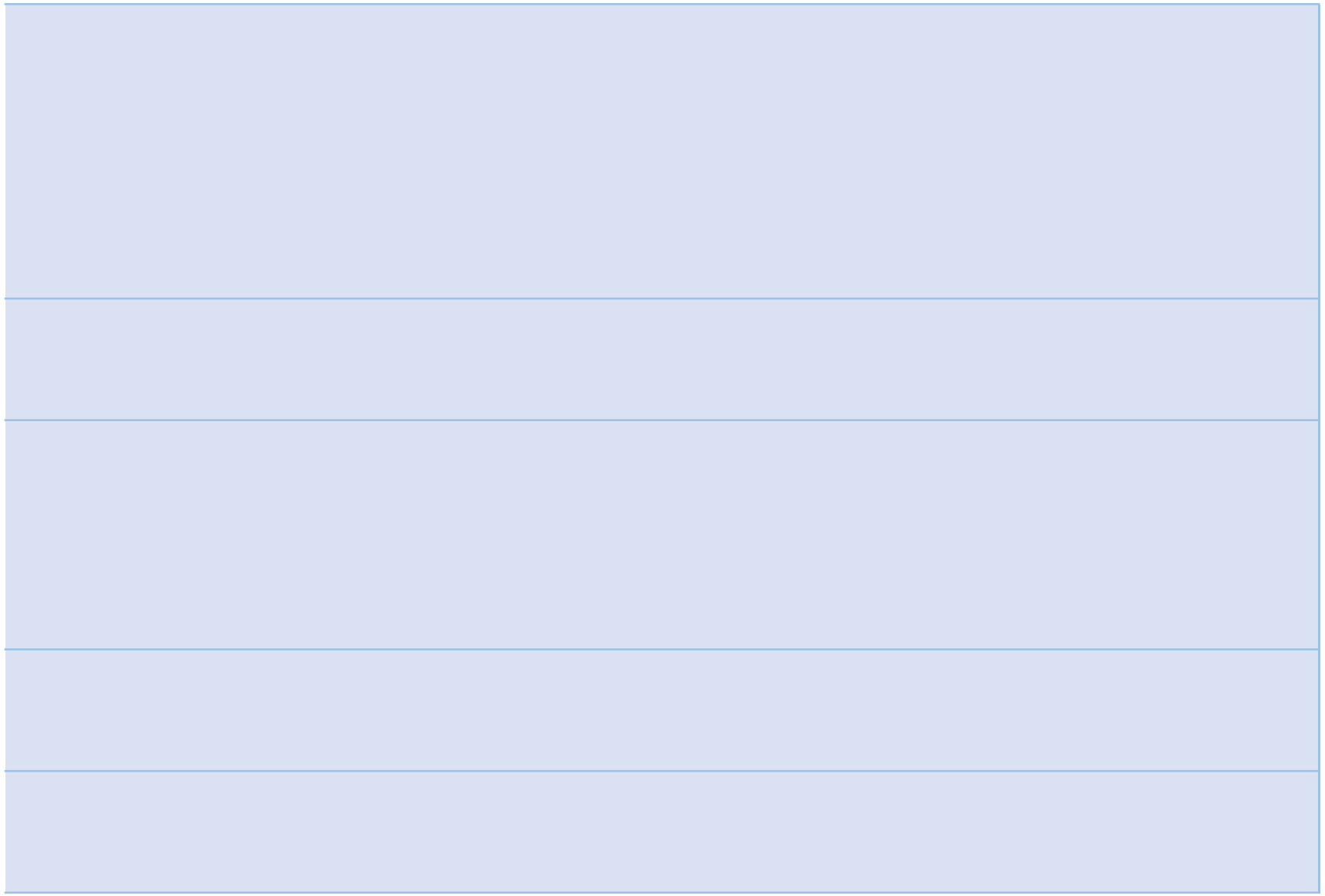
8/9/2024, 1:27 PM	8/9/2025, 1:27 PM	3/6/2025, 10:21 AM	0c13fd90-068e-4785-8b00-652c6dbe0445
12/9/2022, 3:18 PM	12/9/2023, 3:18 PM	3/6/2025, 10:06 AM	29be4854-f18d-45f4-b5b4-cf3c9613c4b5
7/30/2024, 5:49 PM	7/30/2025, 5:49 PM	3/6/2025, 10:06 AM	fe96bbd5-0cc4-4c18-b796-4f75b5e5d44f
5/29/2024, 8:23 PM	5/29/2025, 8:23 PM	3/6/2025, 10:05 AM	0ebe3fad-f94b-4f2e-a85f-962d536acca5

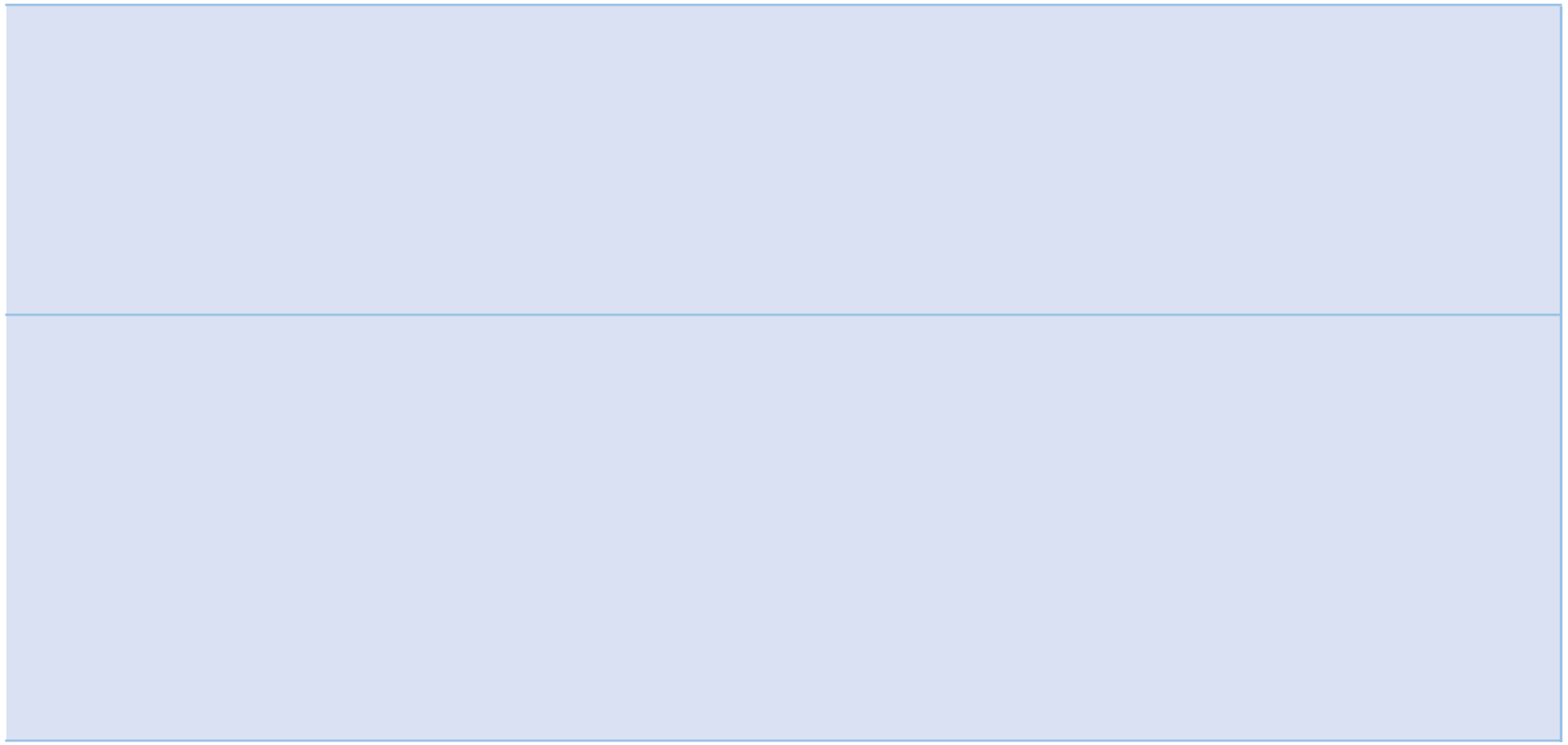
5/13/2024, 6:48 PM	5/13/2025, 6:48 PM	3/6/2025, 10:04 AM	543d3cca-3dd6-4024-b6ce-79ea12b914e3	
5/29/2024, 12:35 PM	5/29/2025, 12:35 PM	3/6/2025, 10:03 AM	d10fa4a6-3e38-4523-8275-d4ab8a242eb1	
12/13/2024, 11:26 AM	12/13/2025, 11:26 AM	3/6/2025, 10:01 AM	eb060e07-61bb-4b3e-a317-0770716f5b2a	
12/13/2023, 3:10 PM	12/13/2024, 3:10 PM	3/6/2025, 9:59 AM	fa7f4f6c-57d1-46ea-ab62-67a2343591bc	

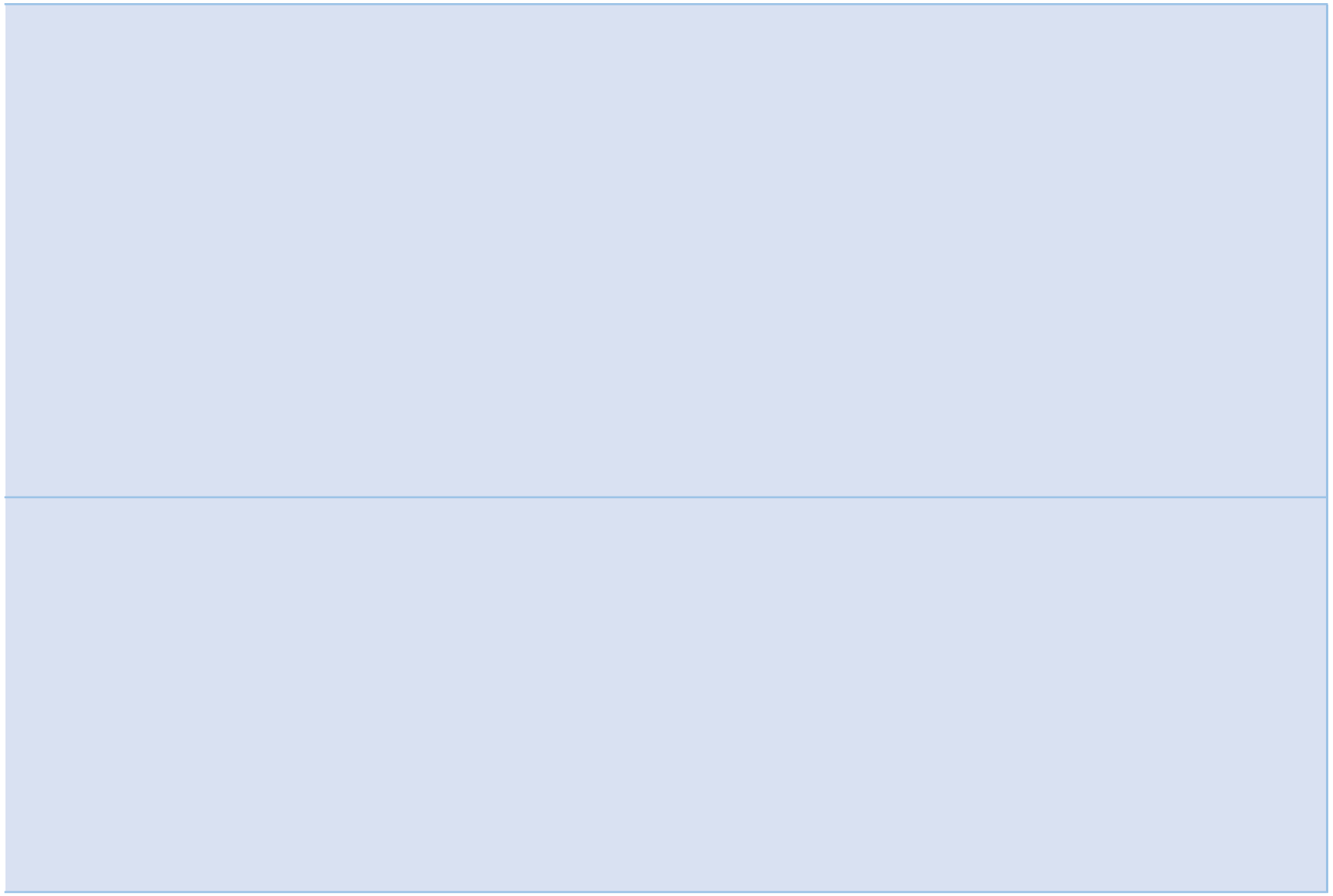
stered trademarks of BlockMark Technologies Ltd. Registered in England with Company Number10821944. VAT Registration Numbe

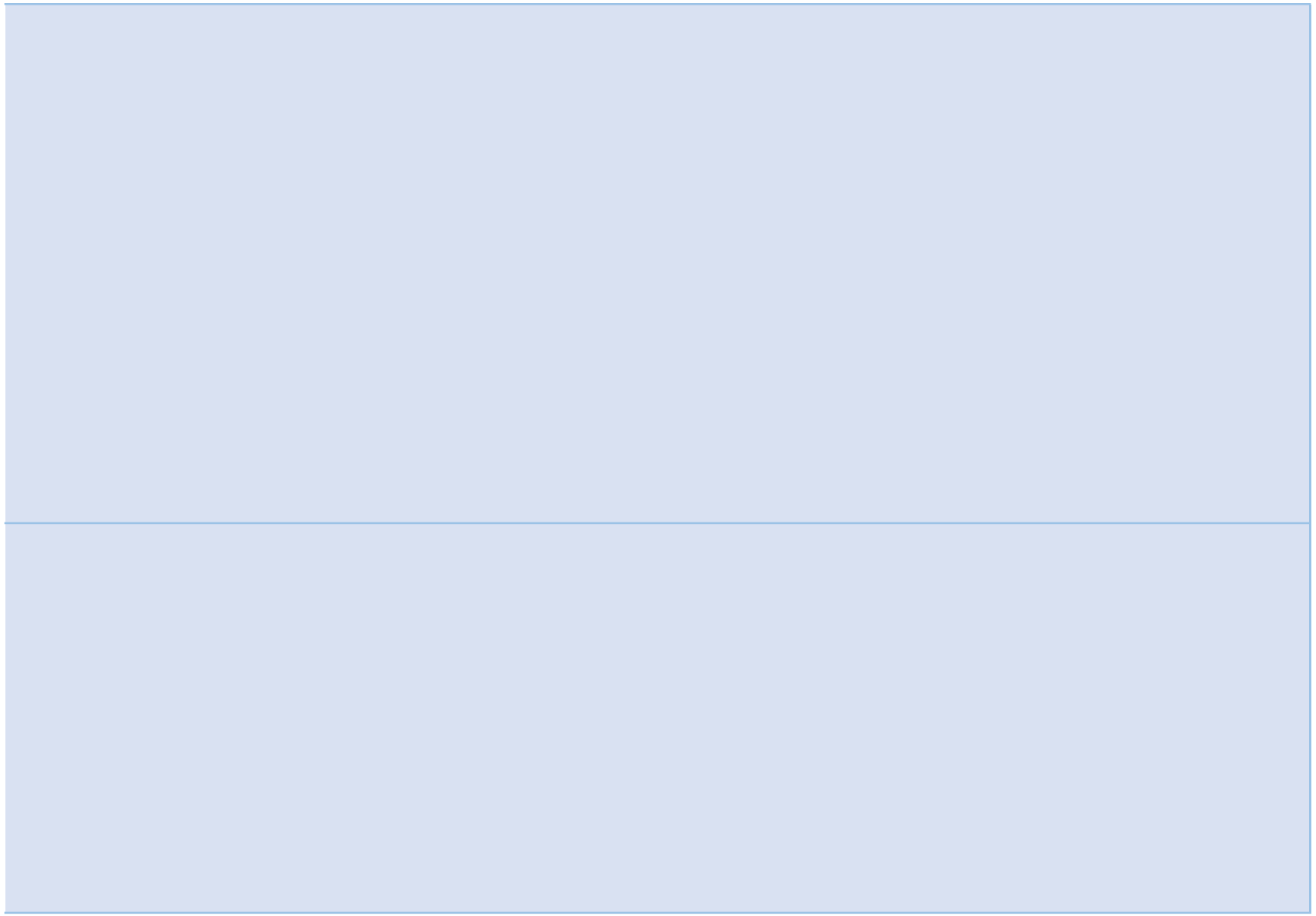


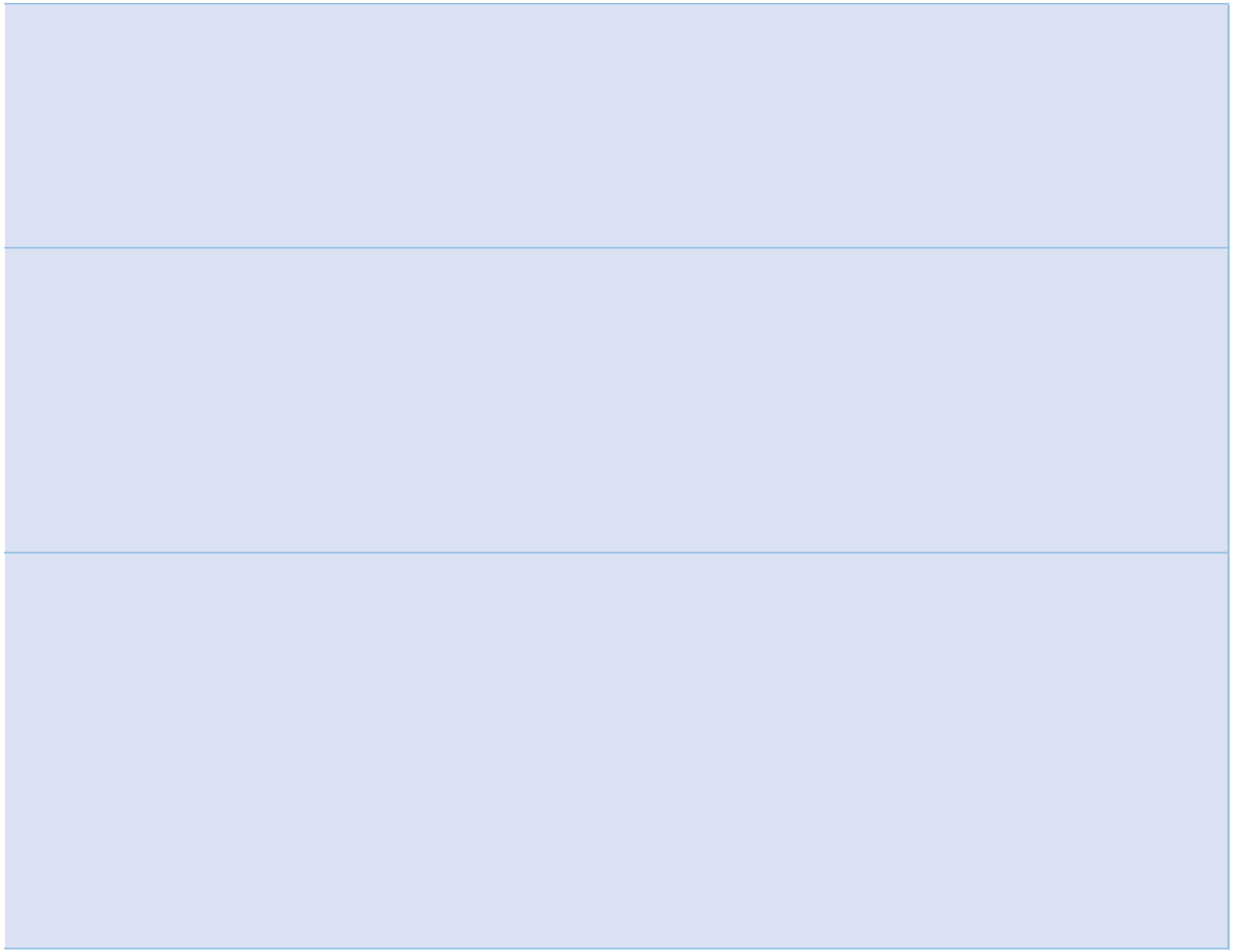


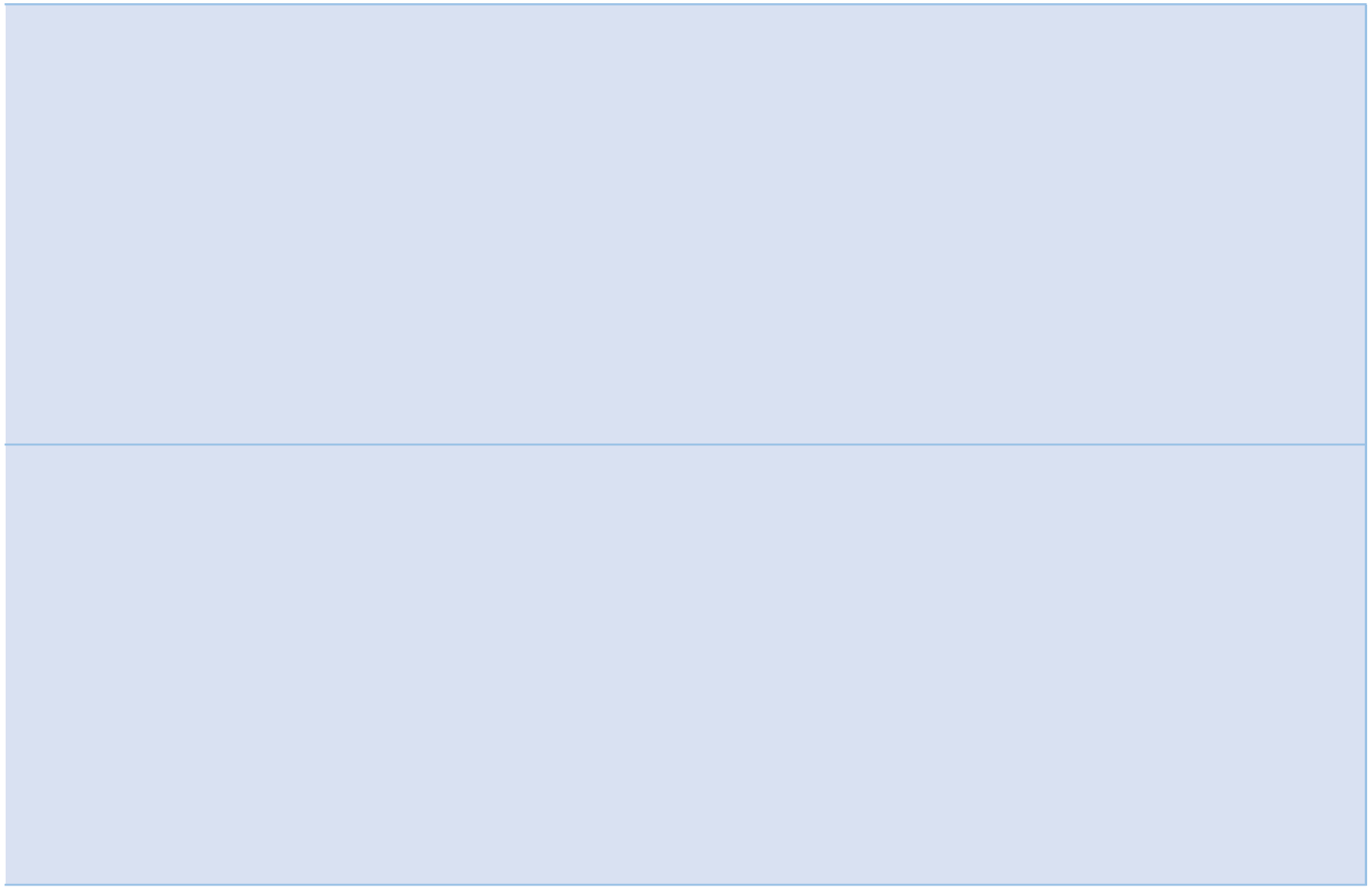


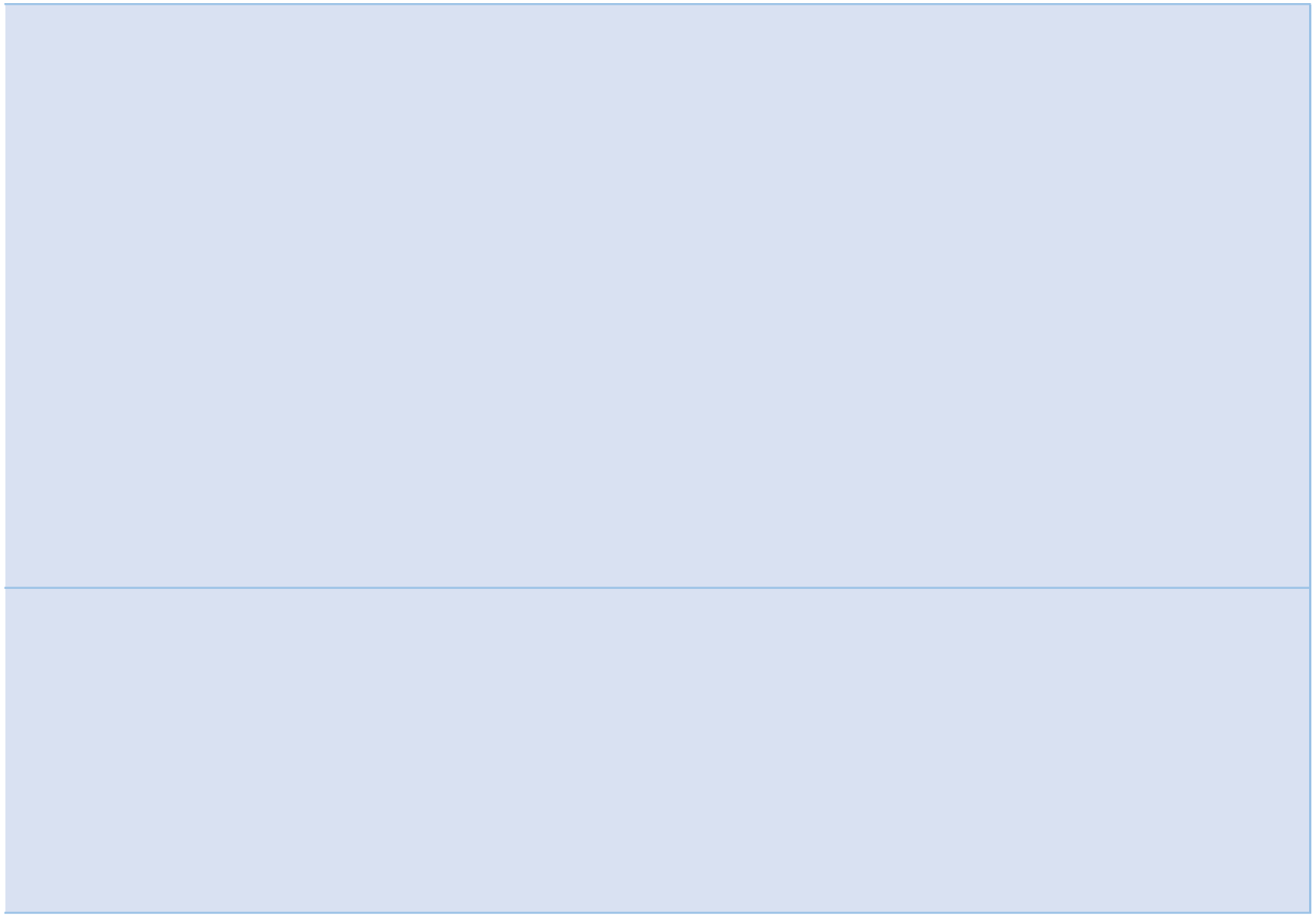


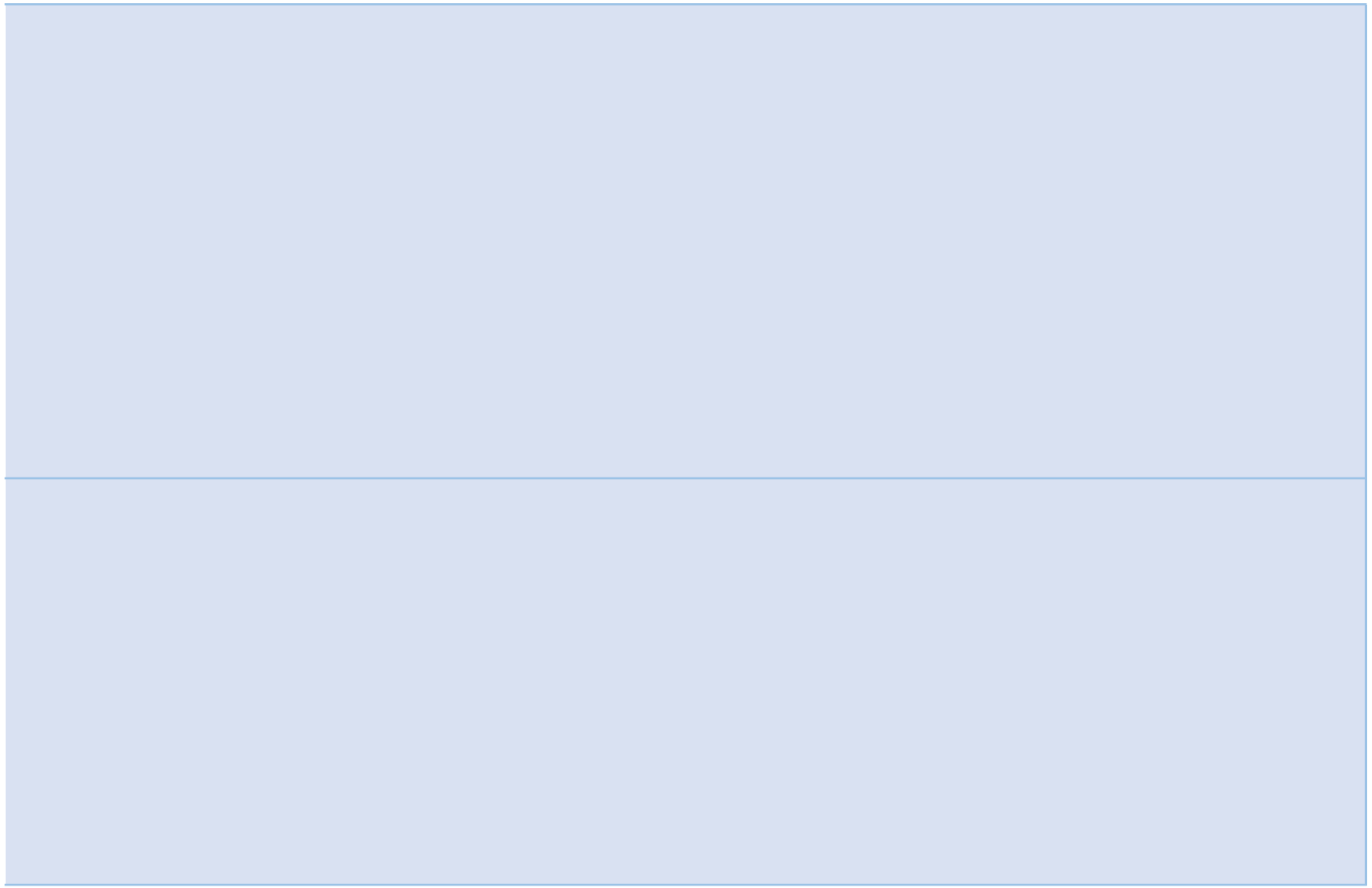


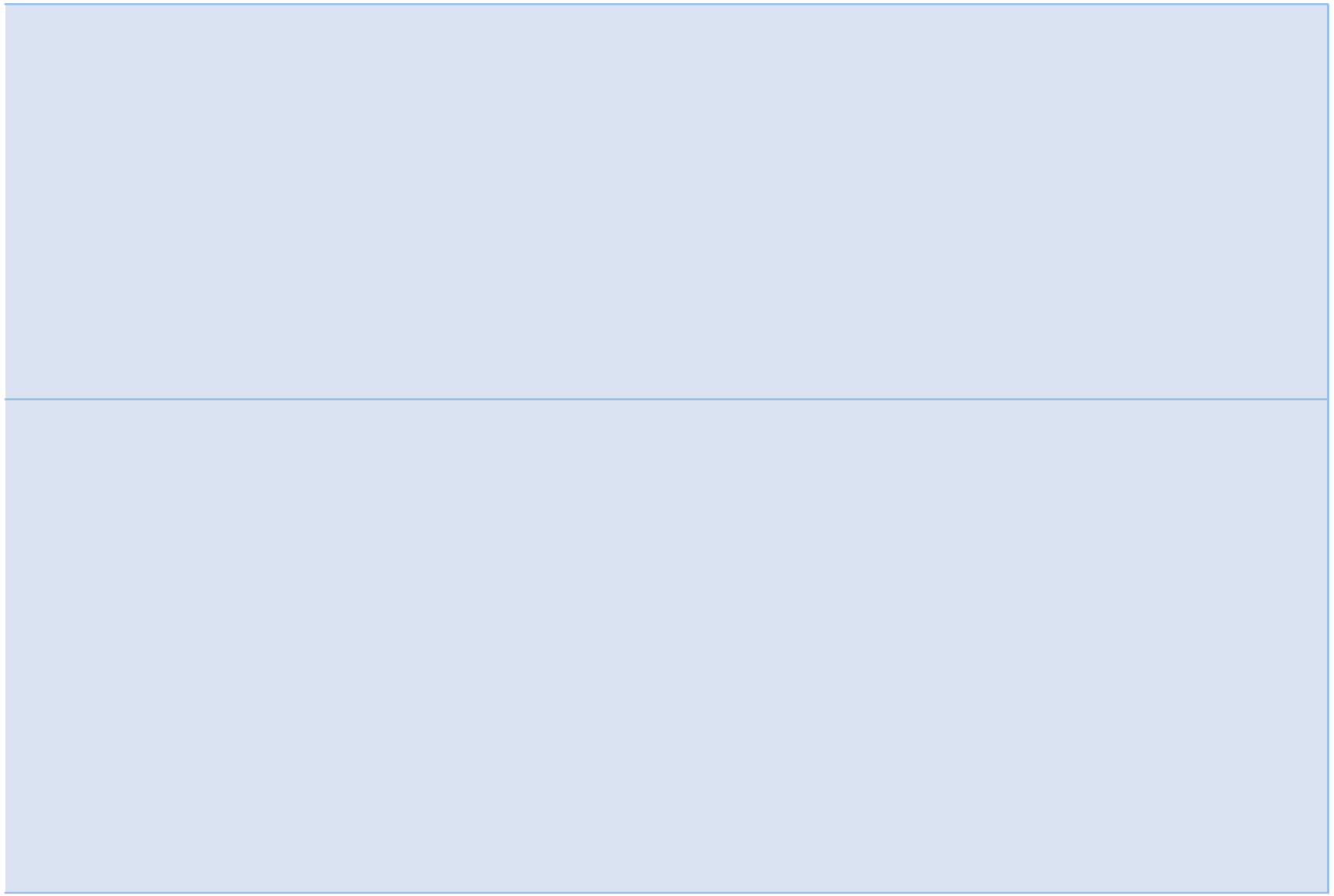


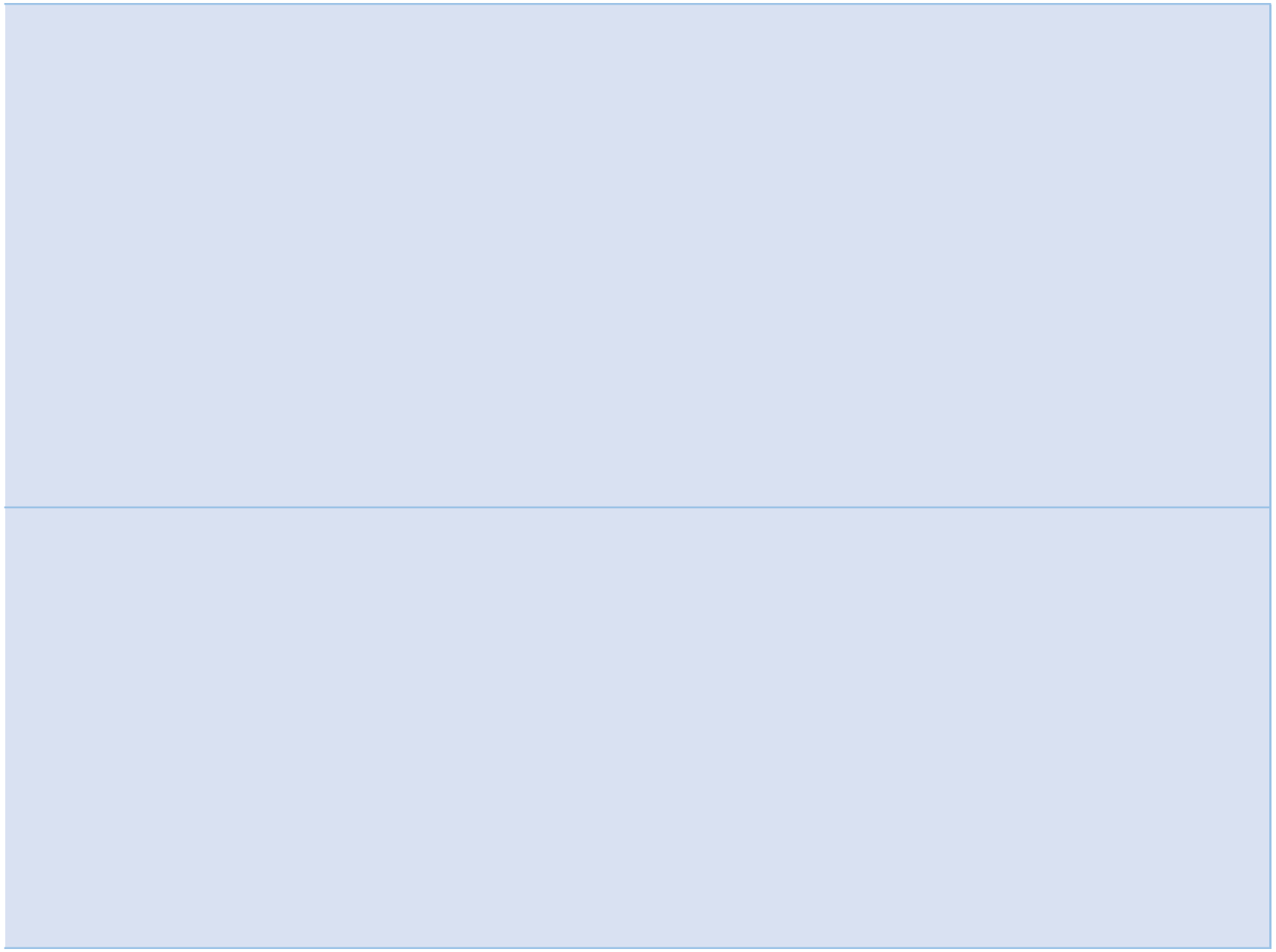


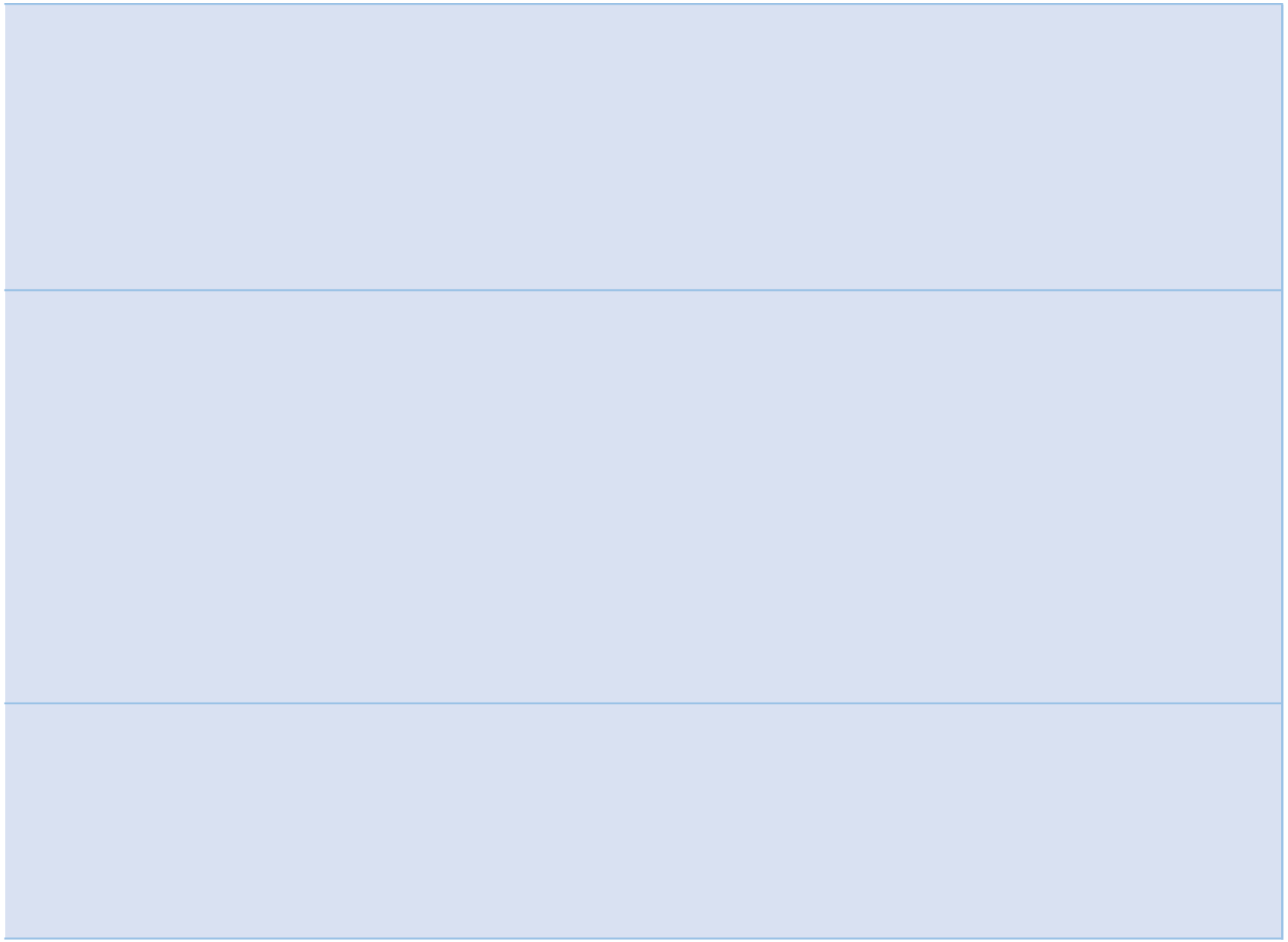


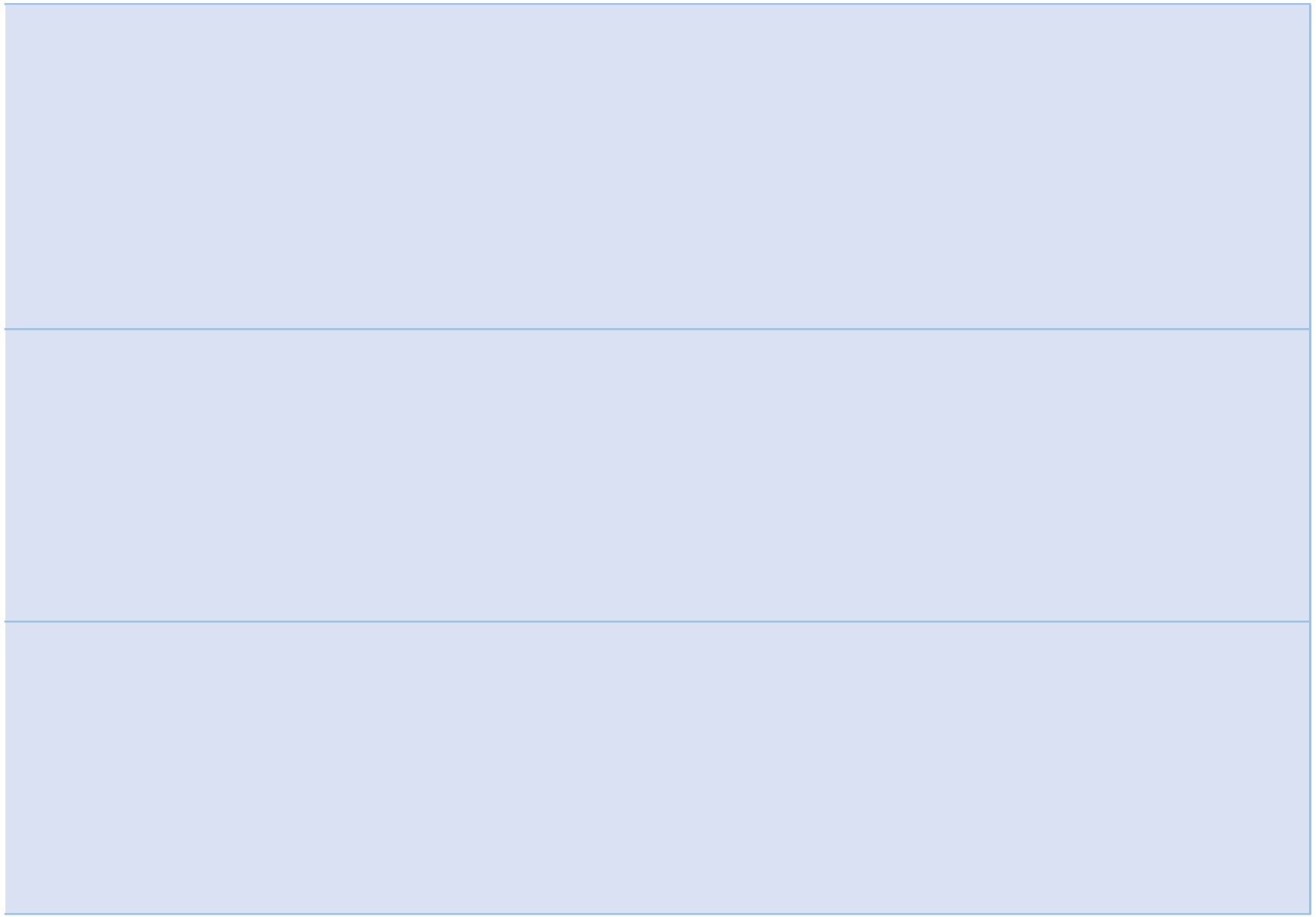


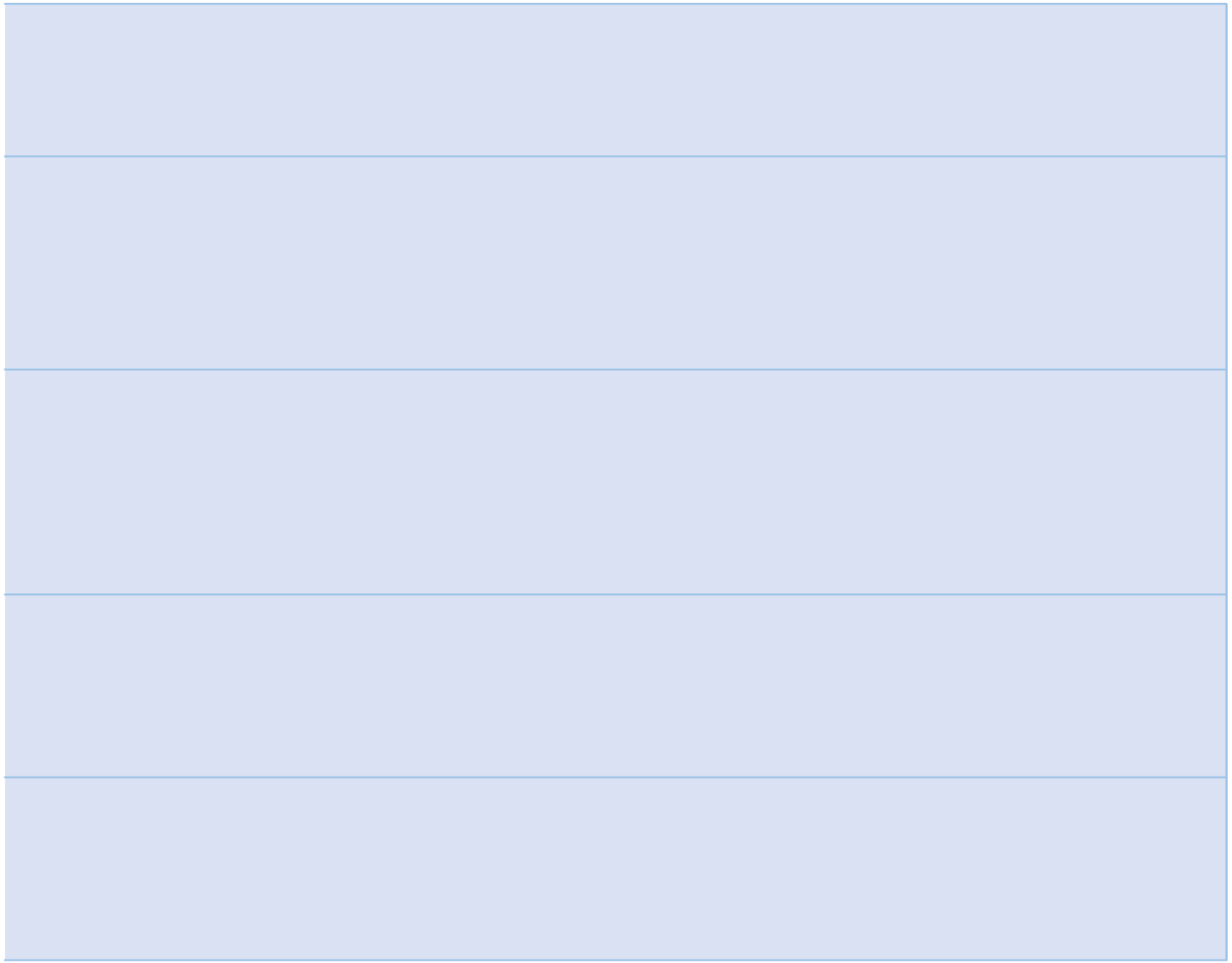


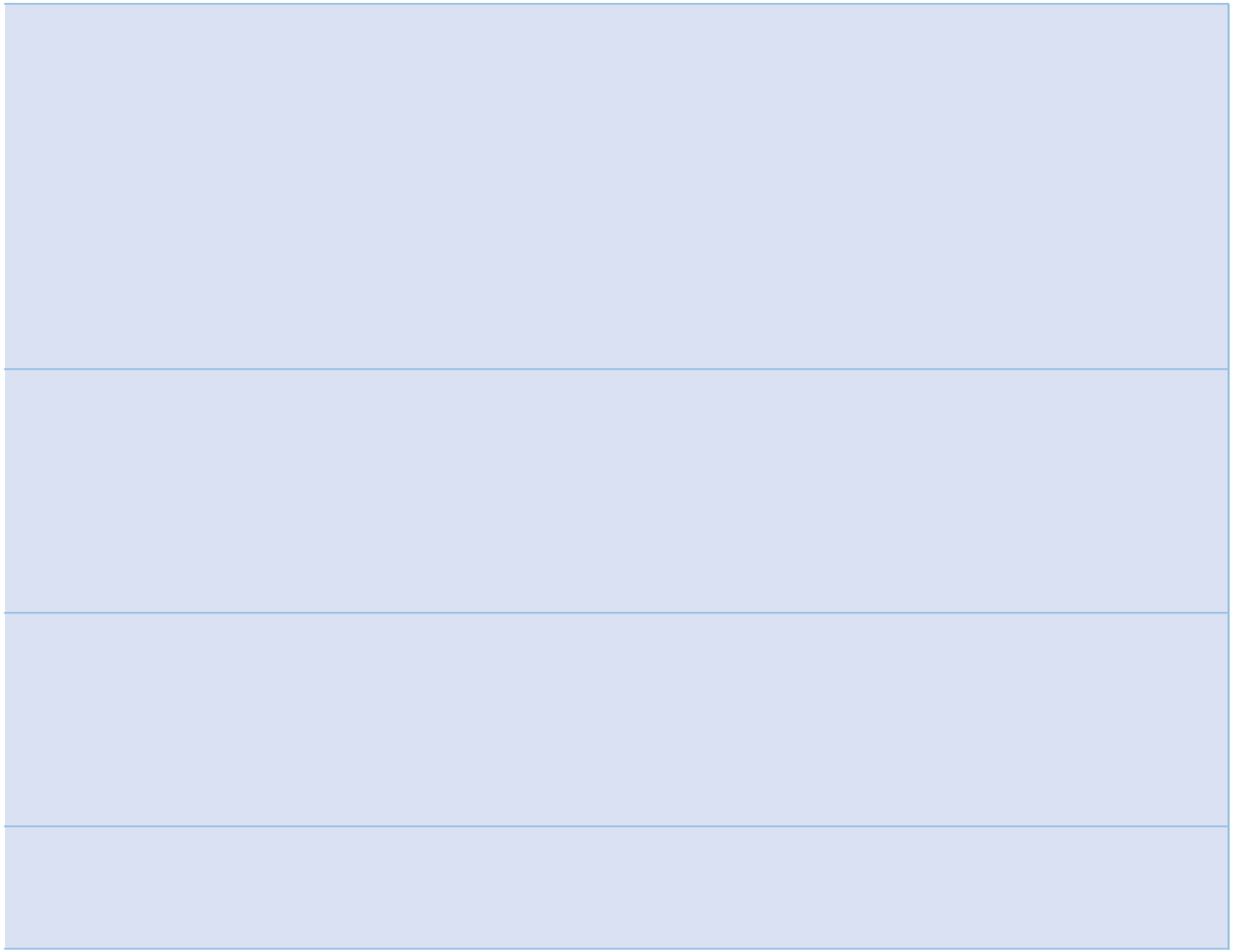


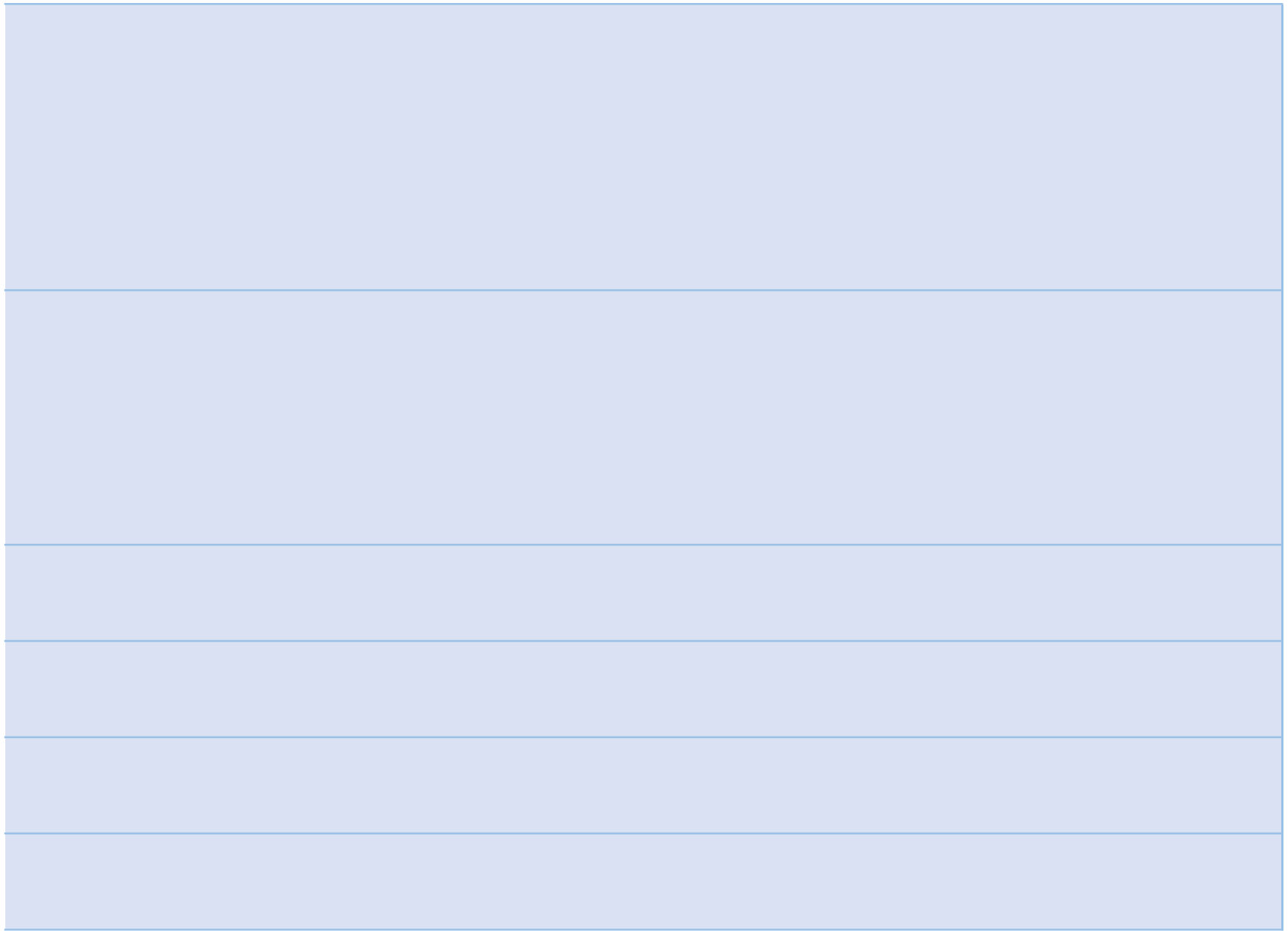


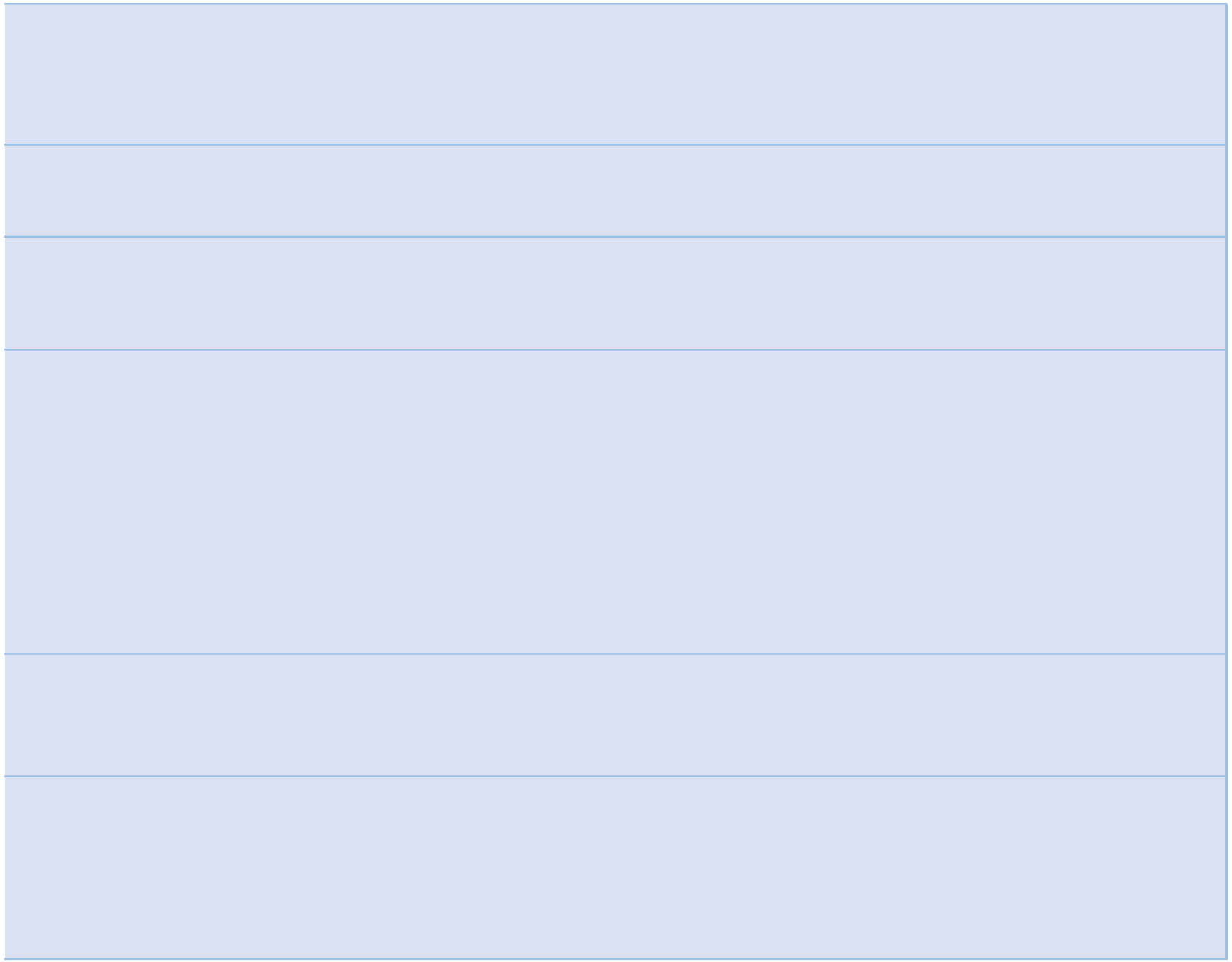


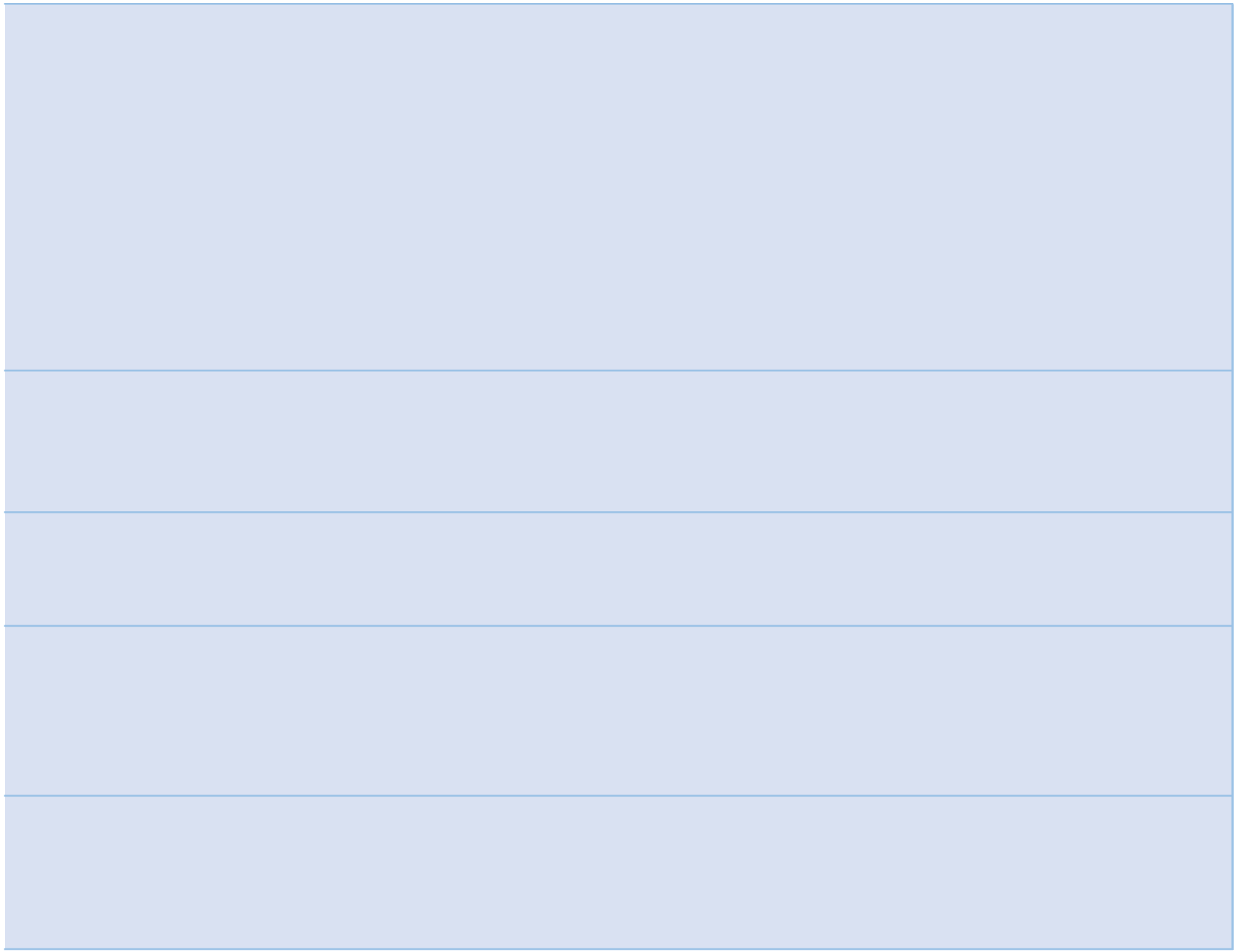


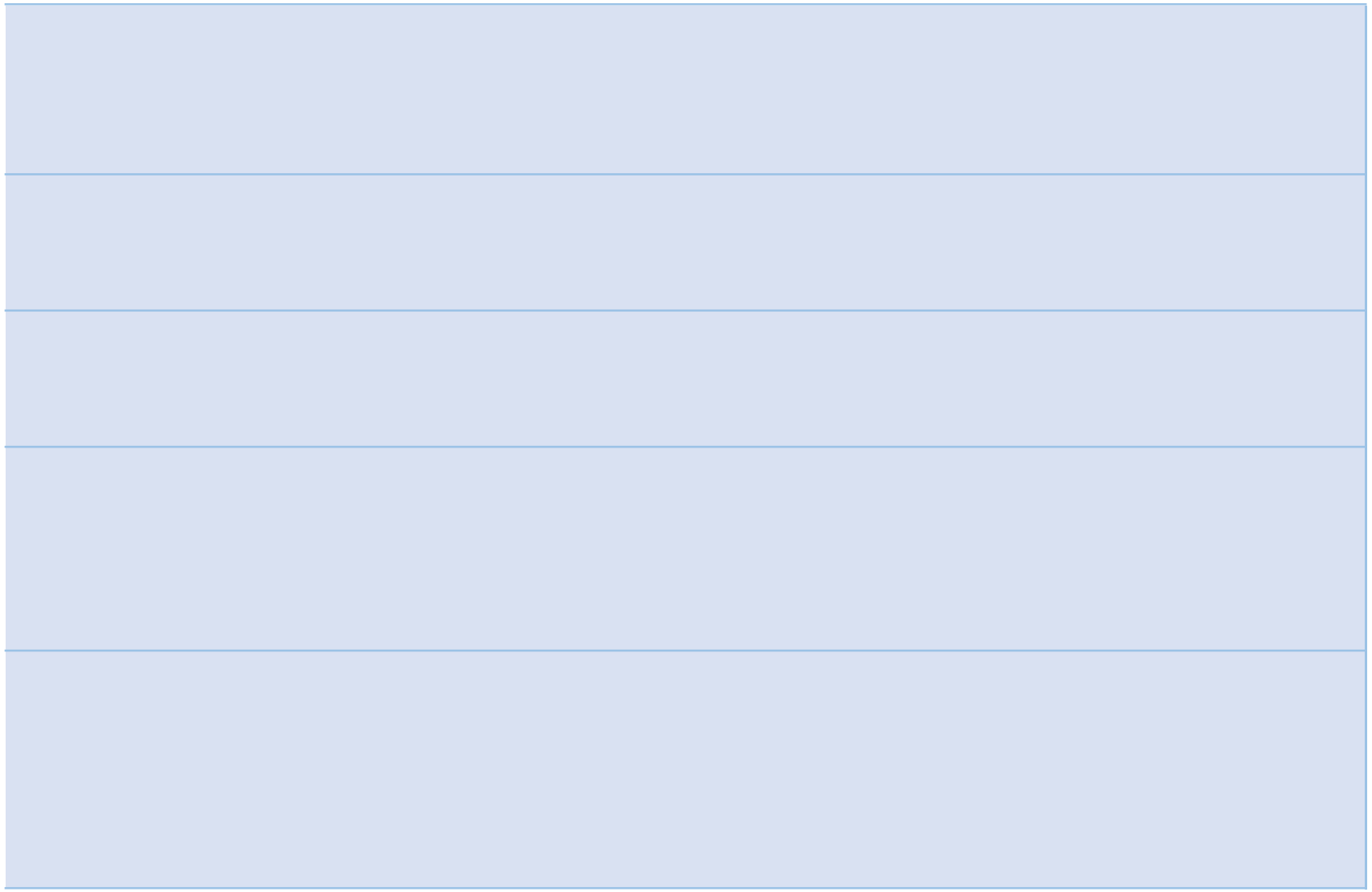


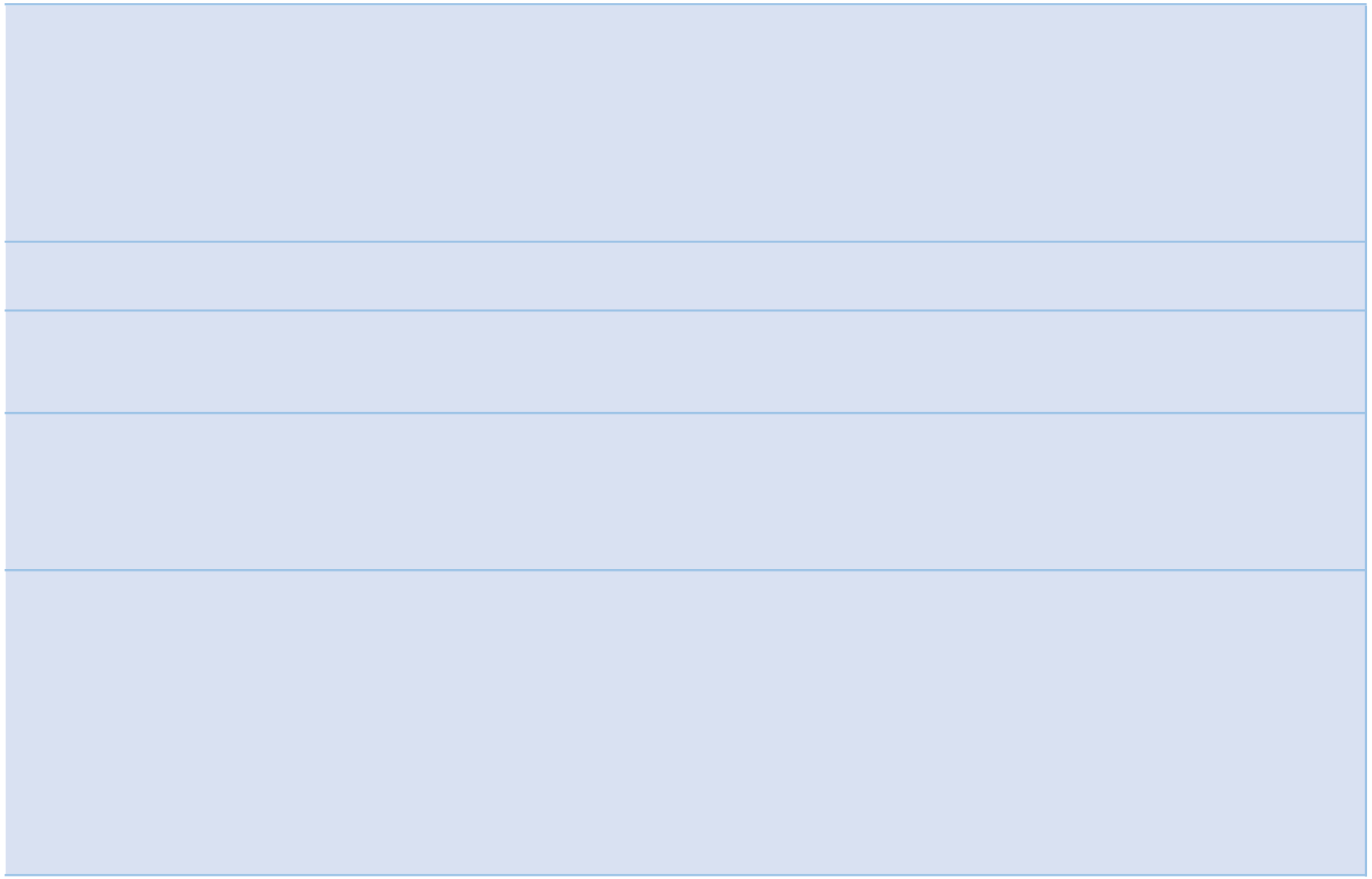


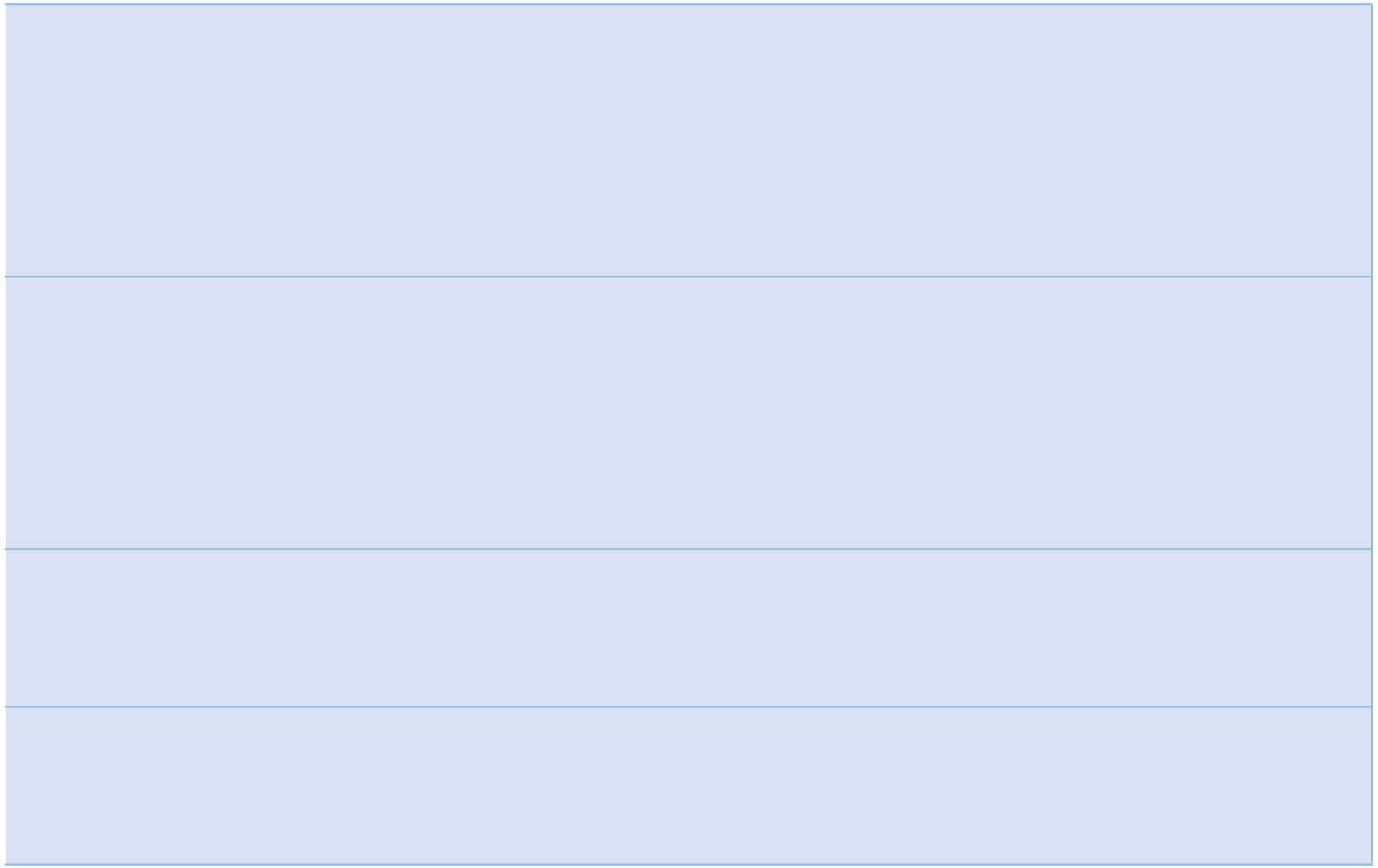


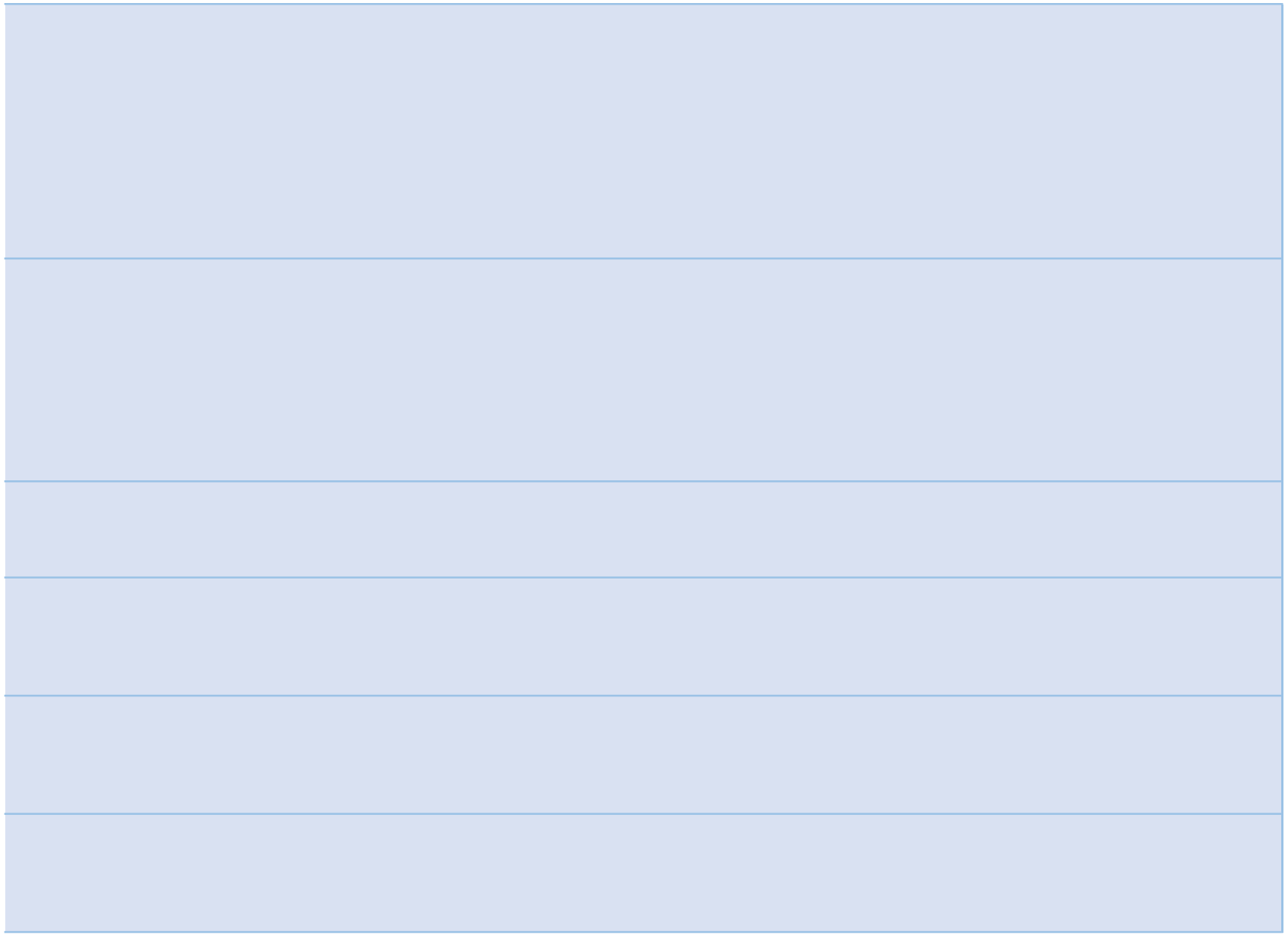


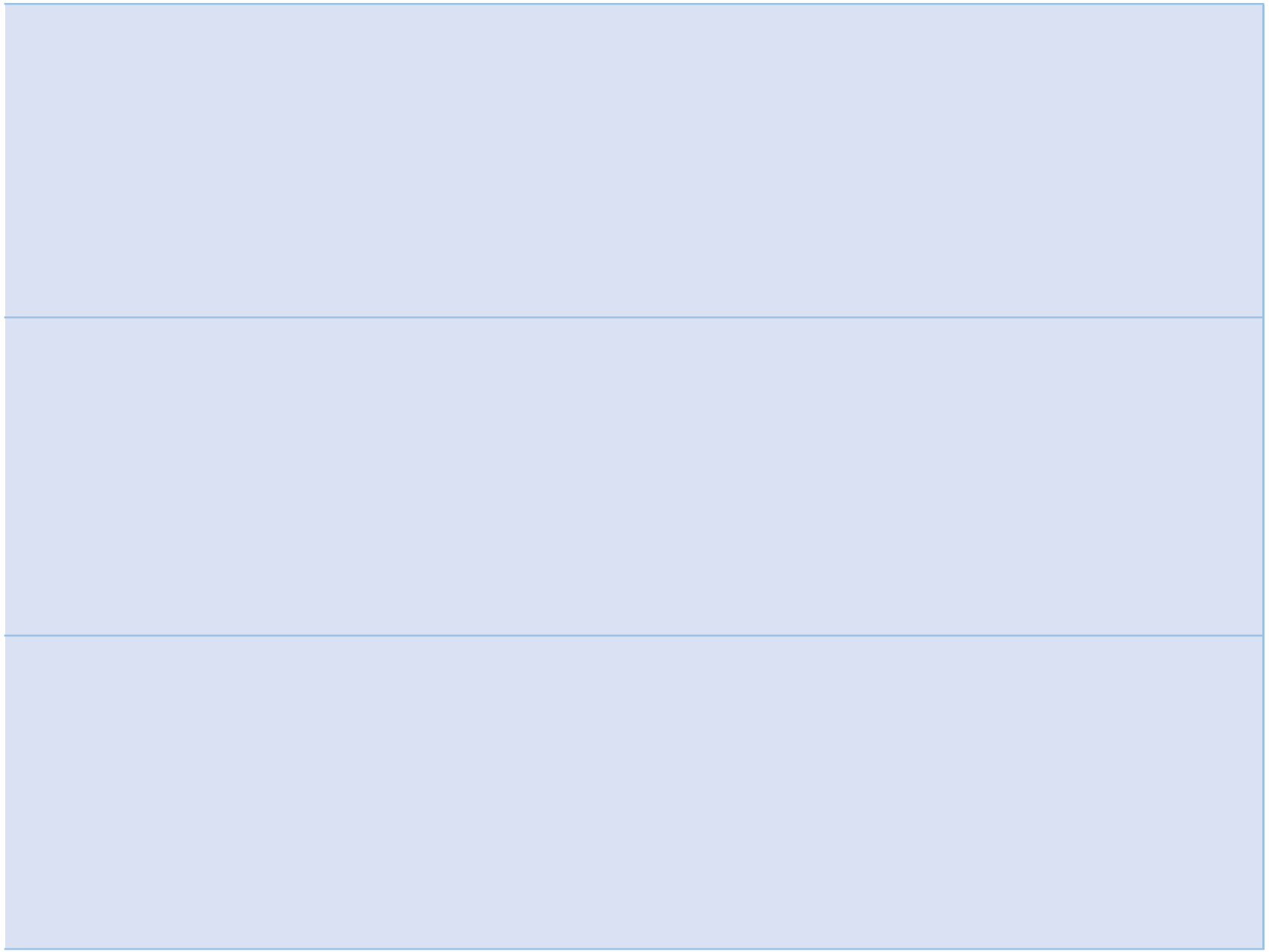


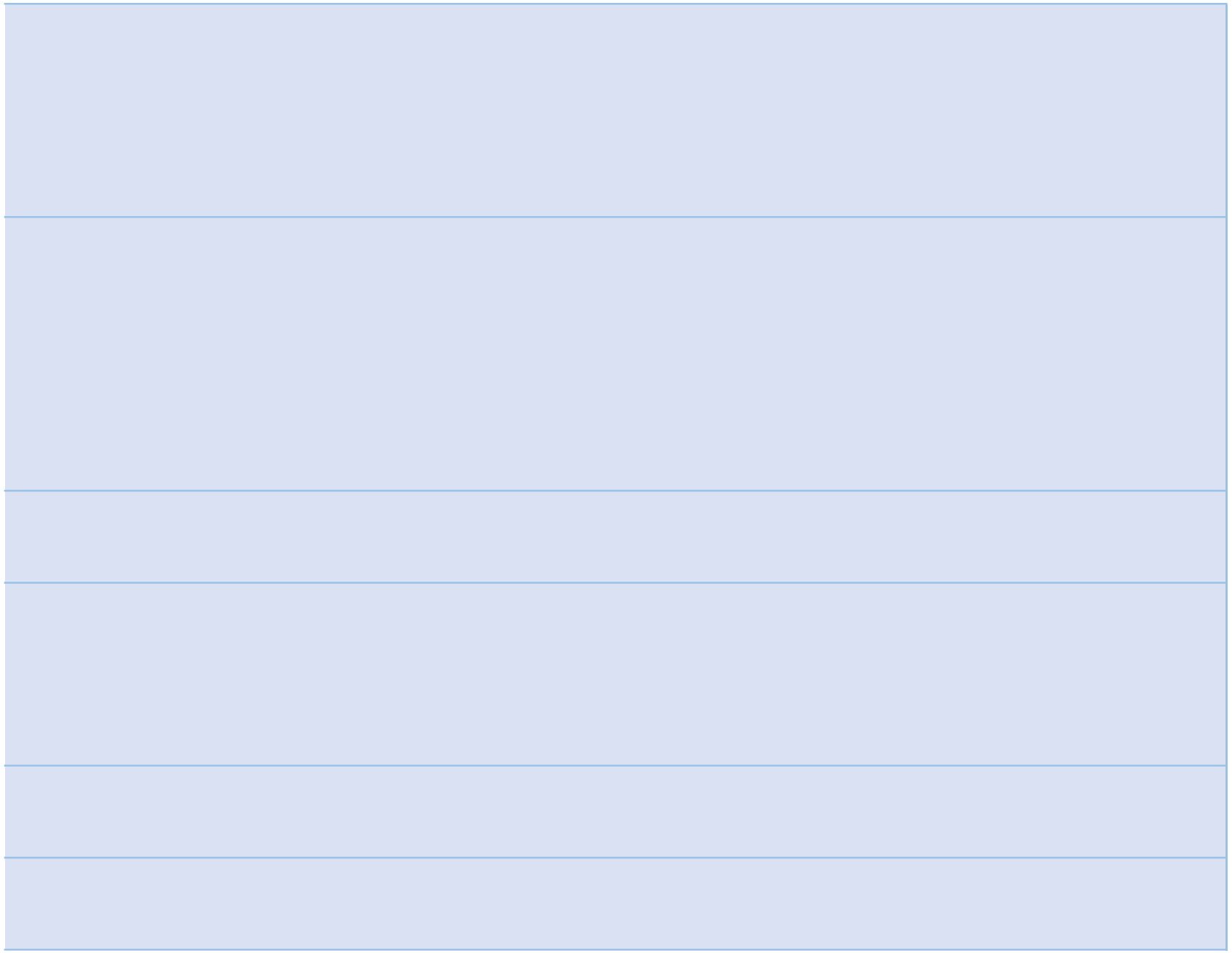


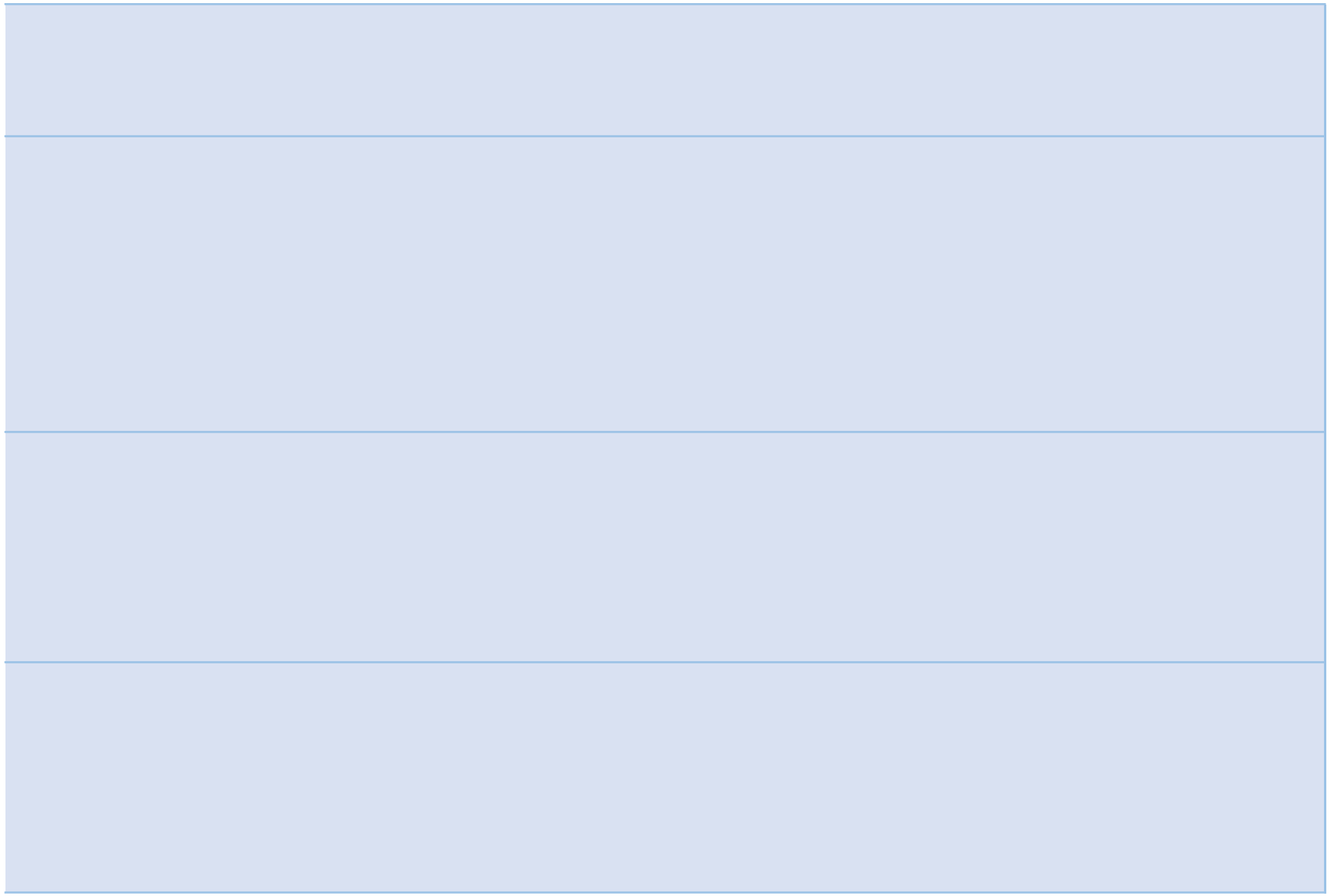


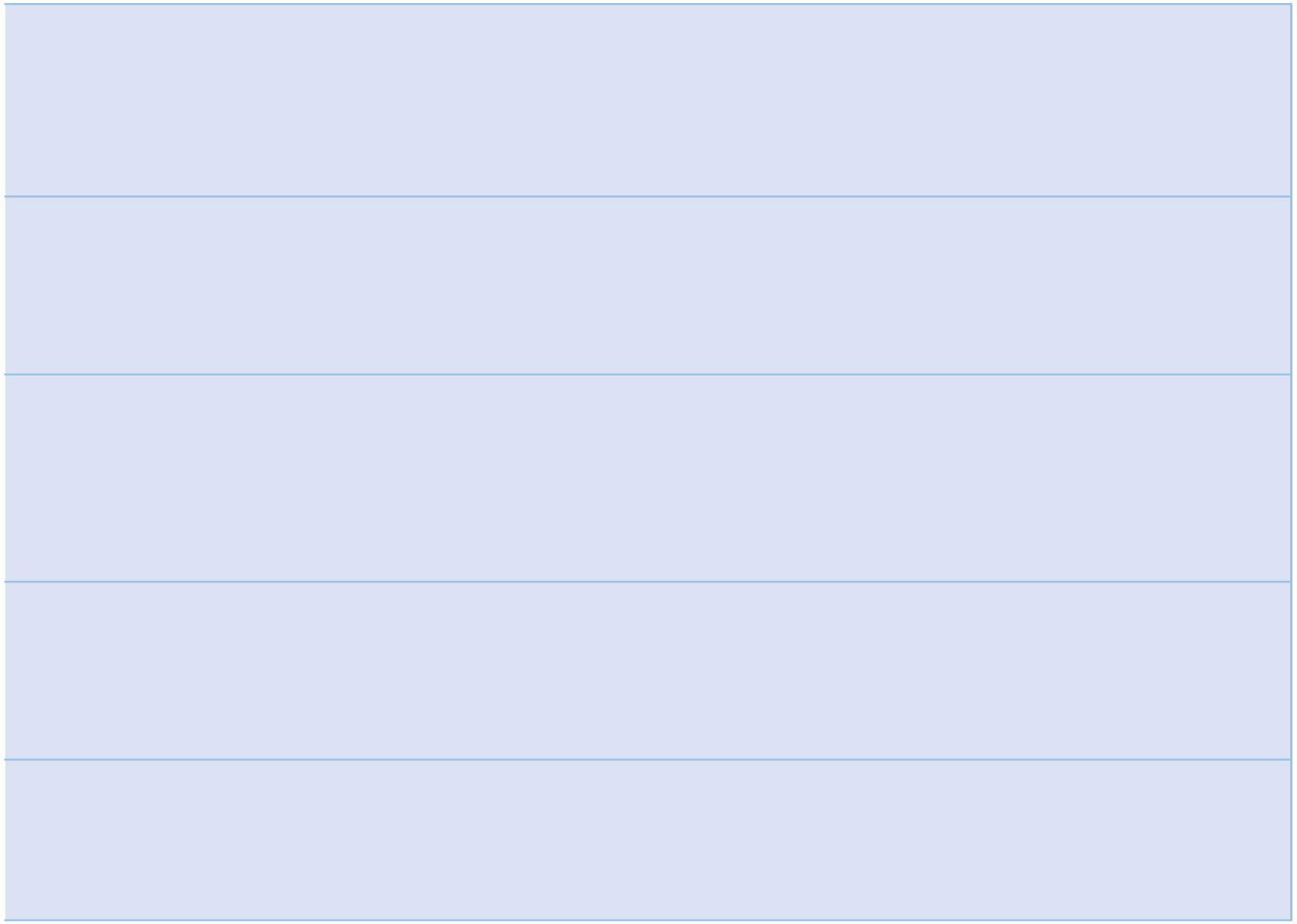


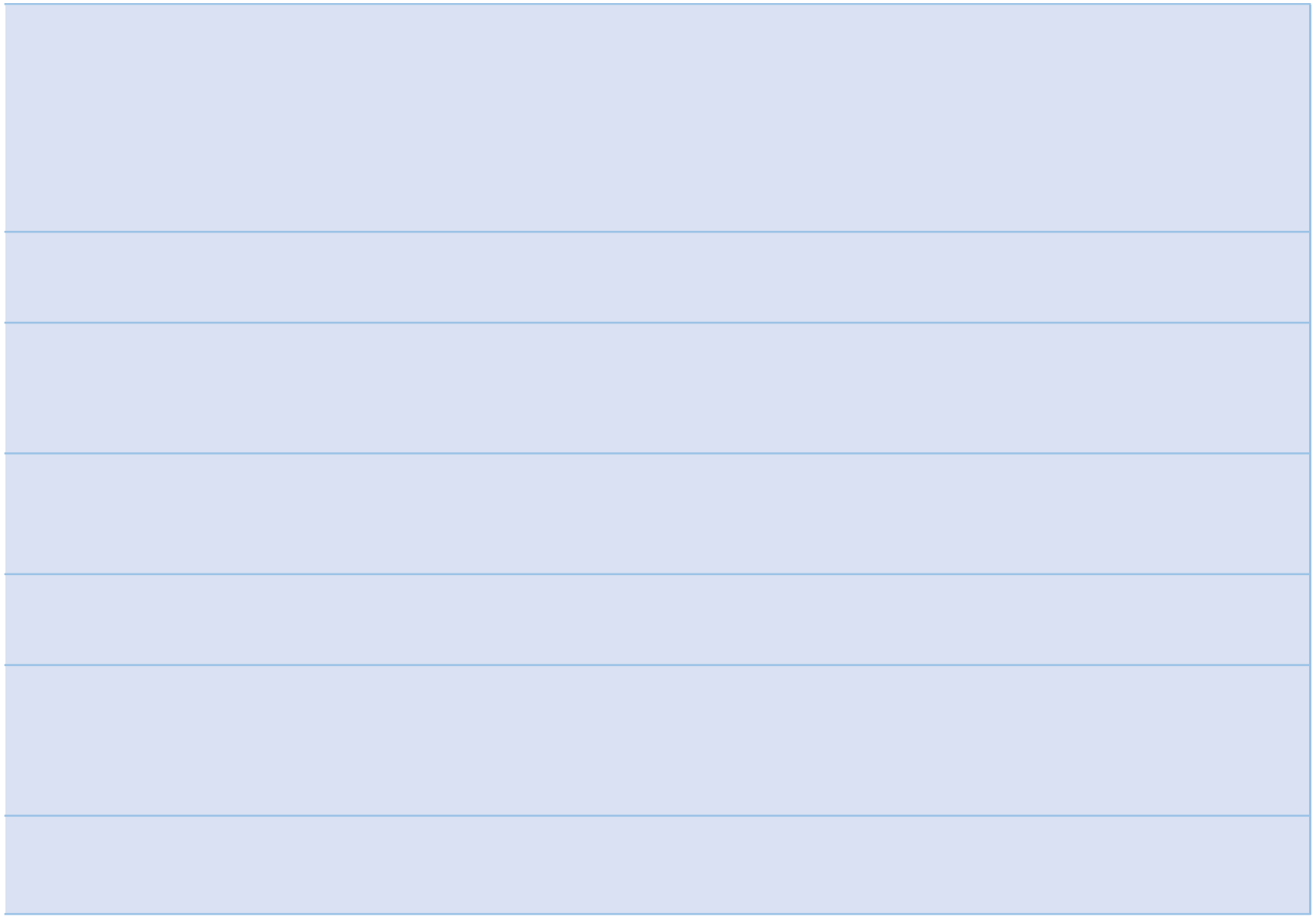


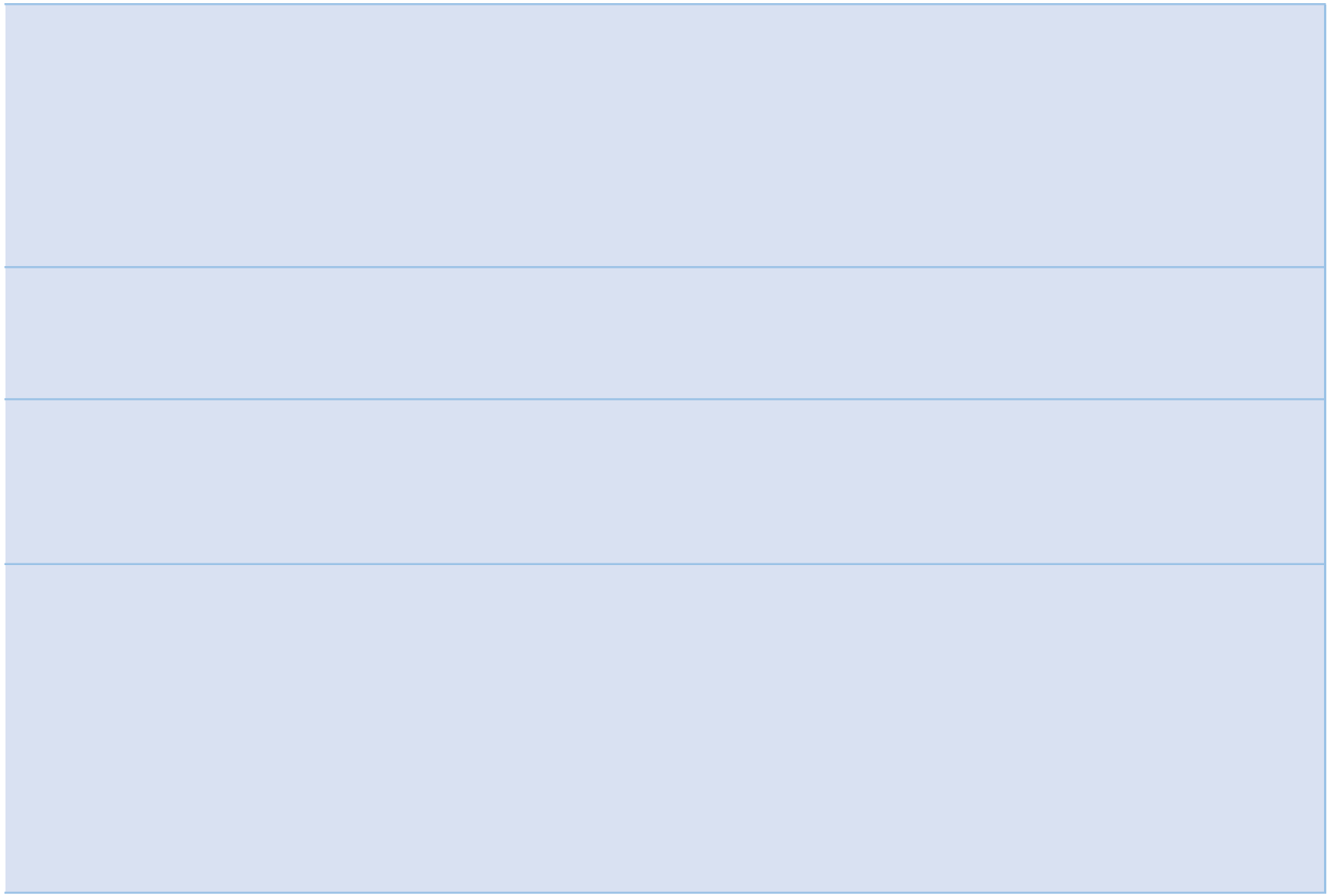


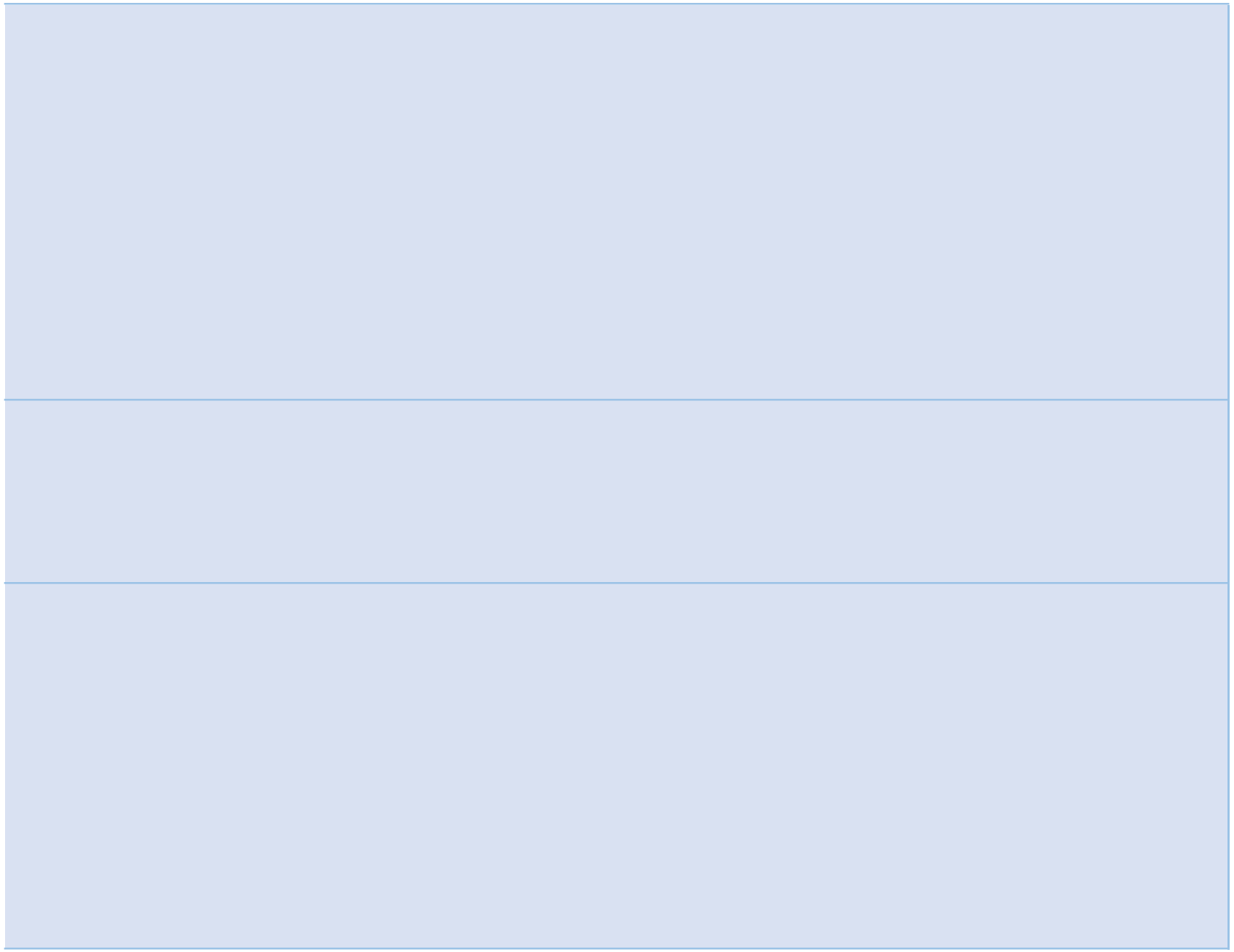


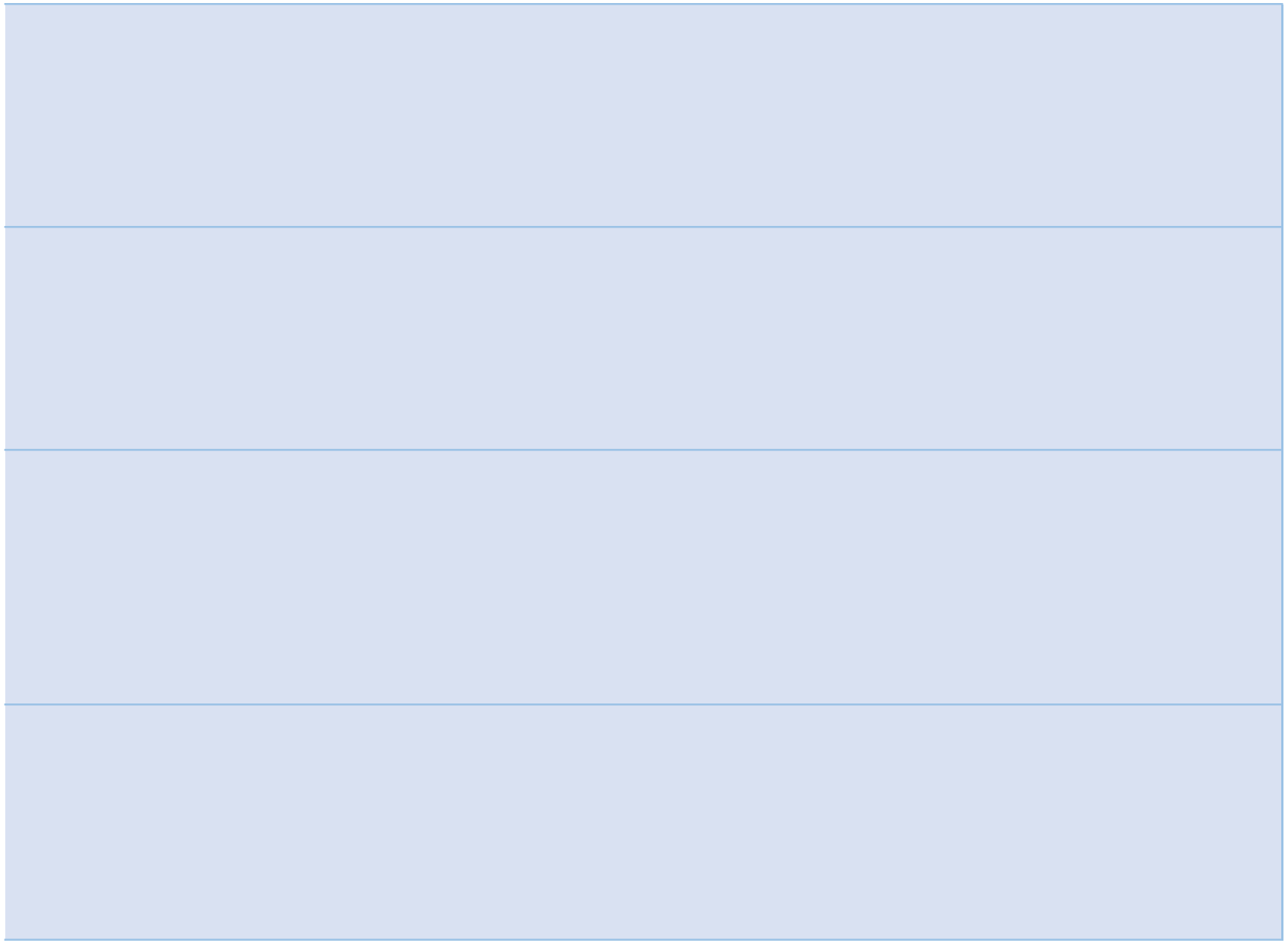


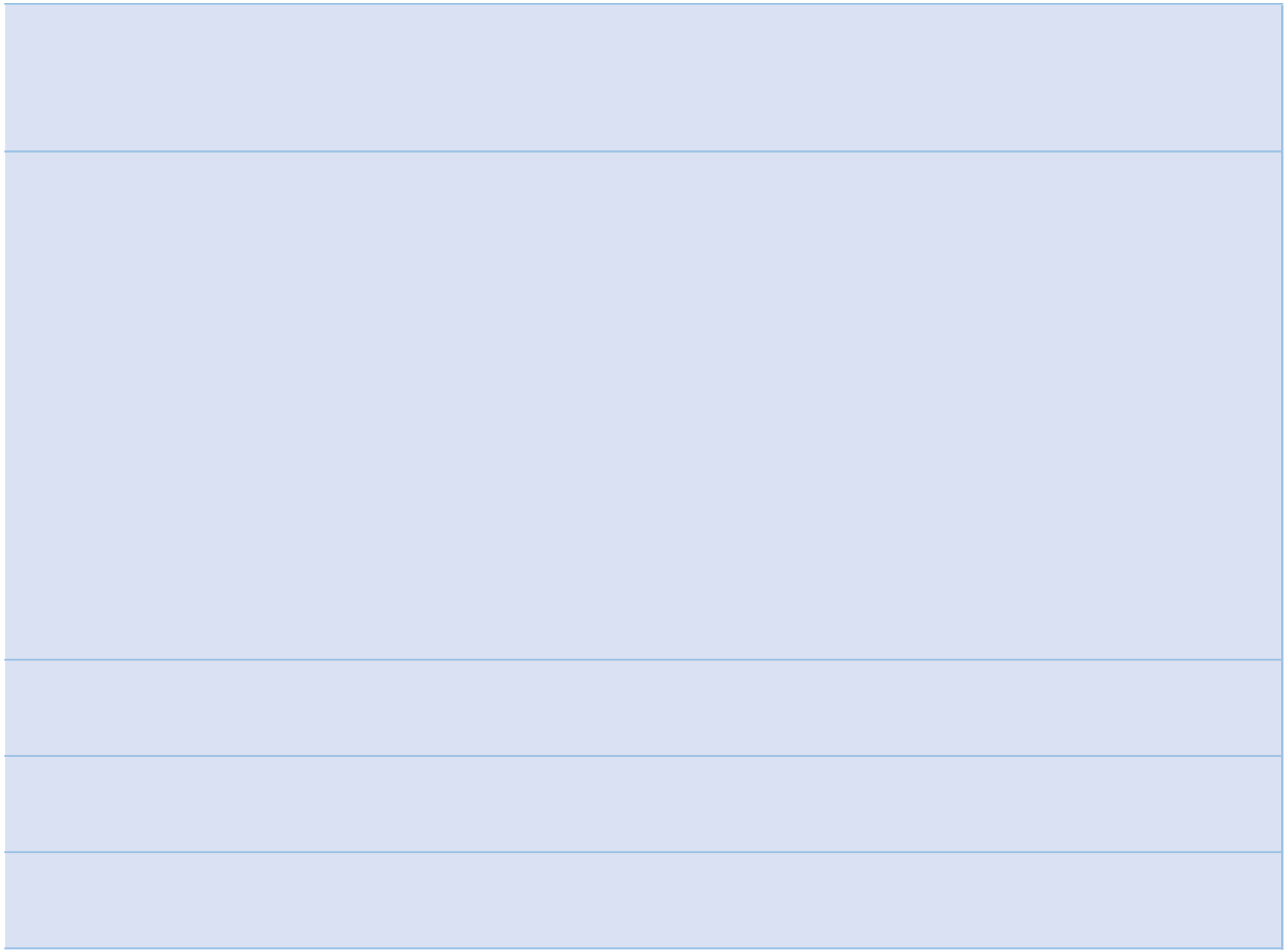


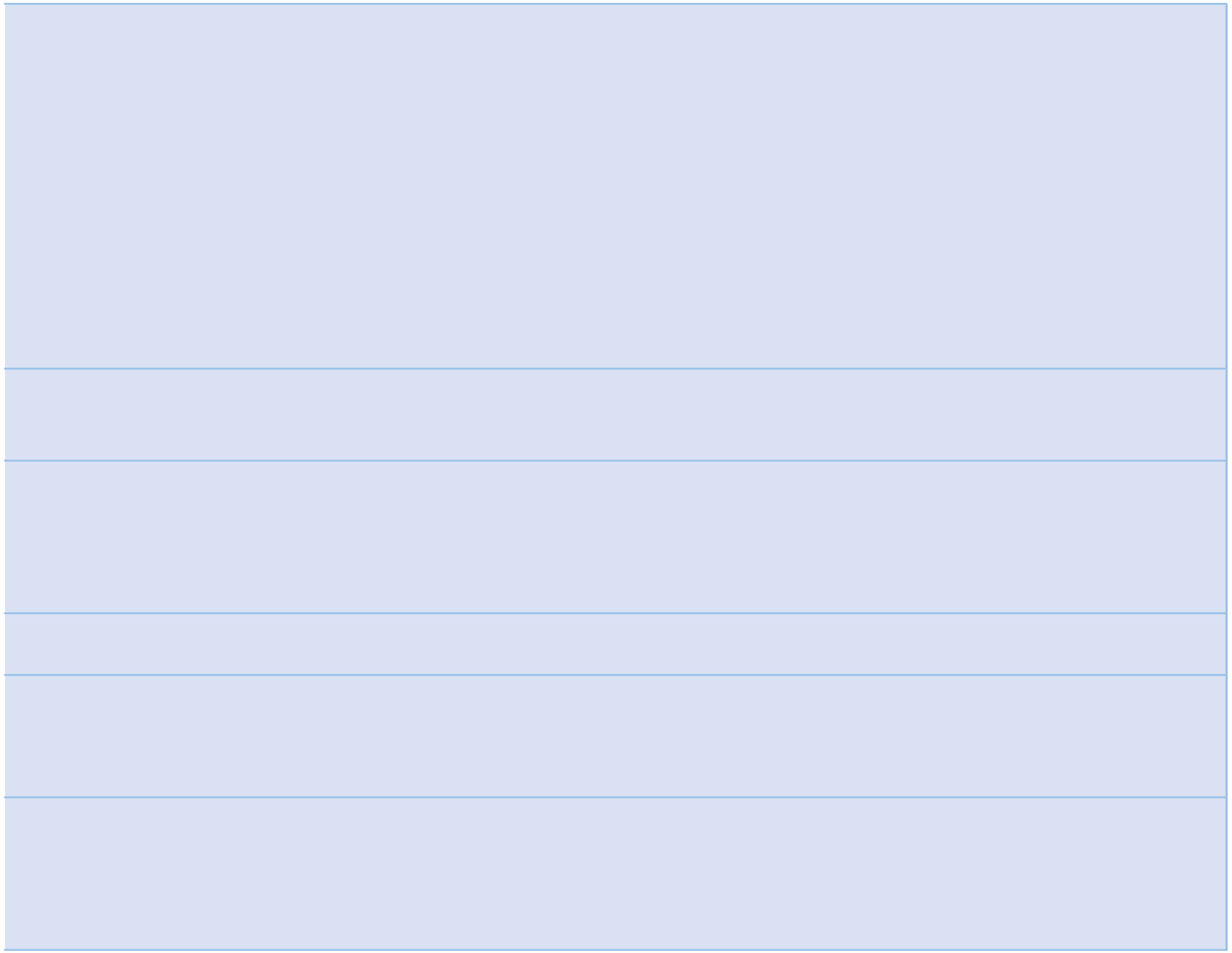


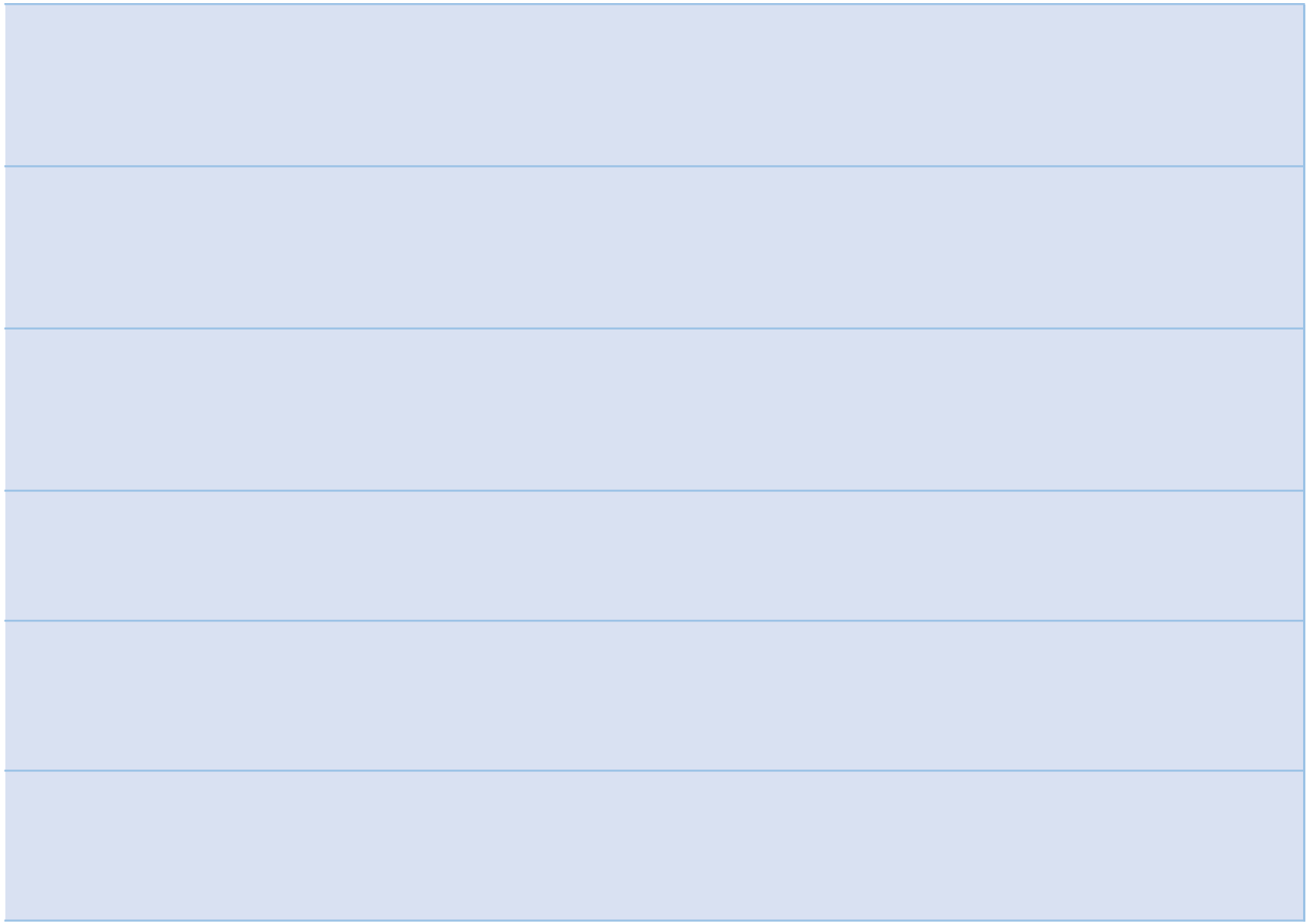


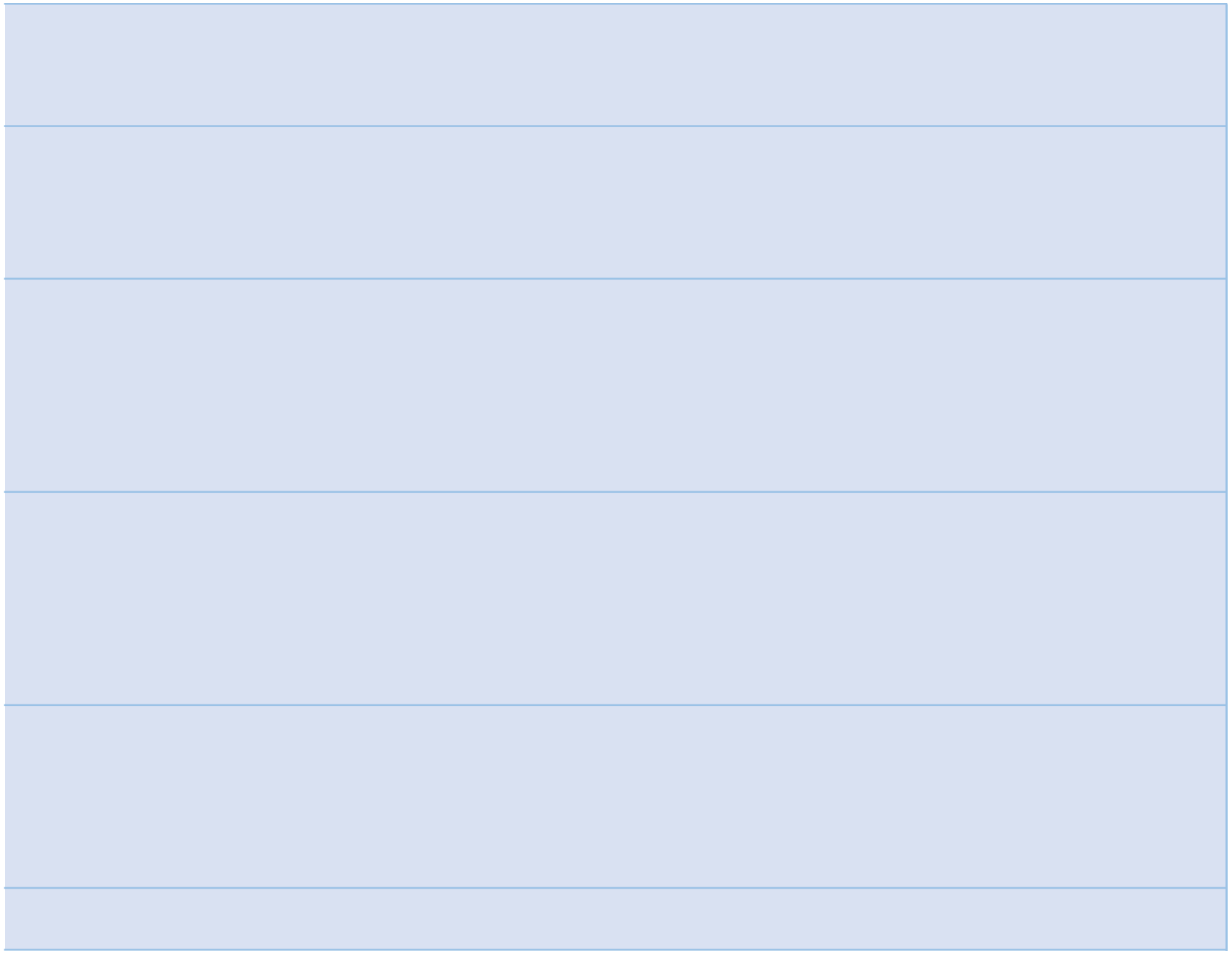


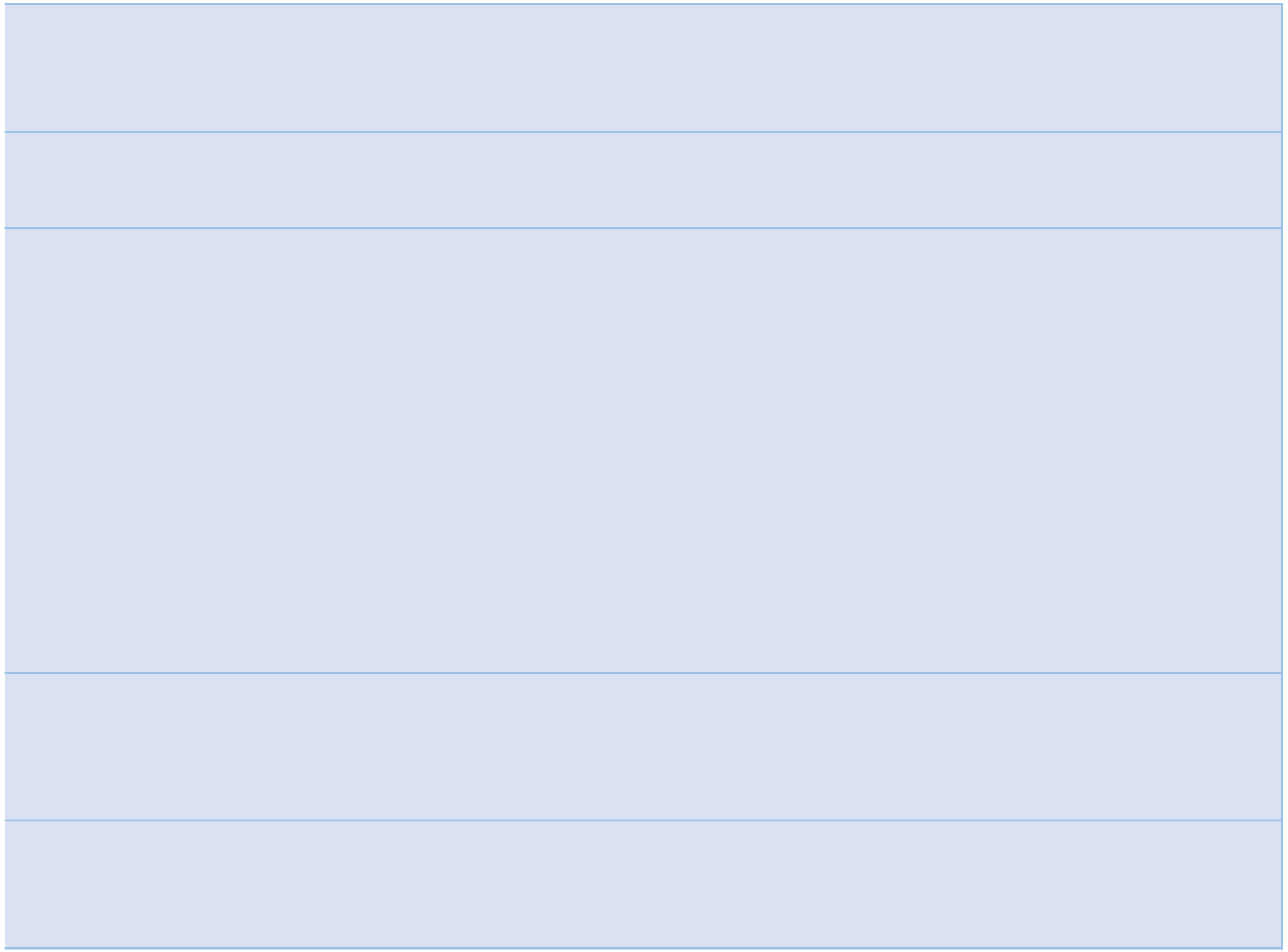


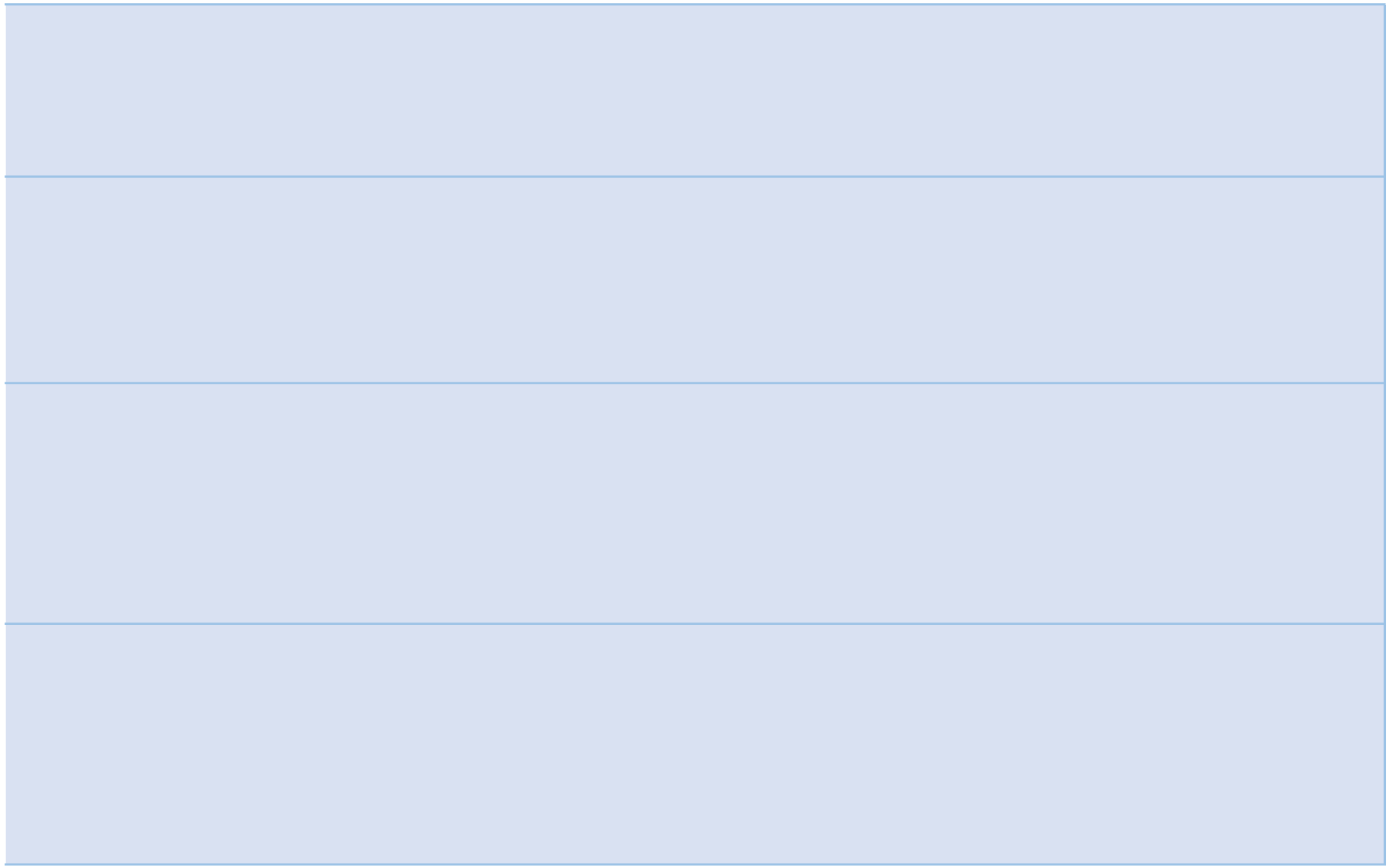


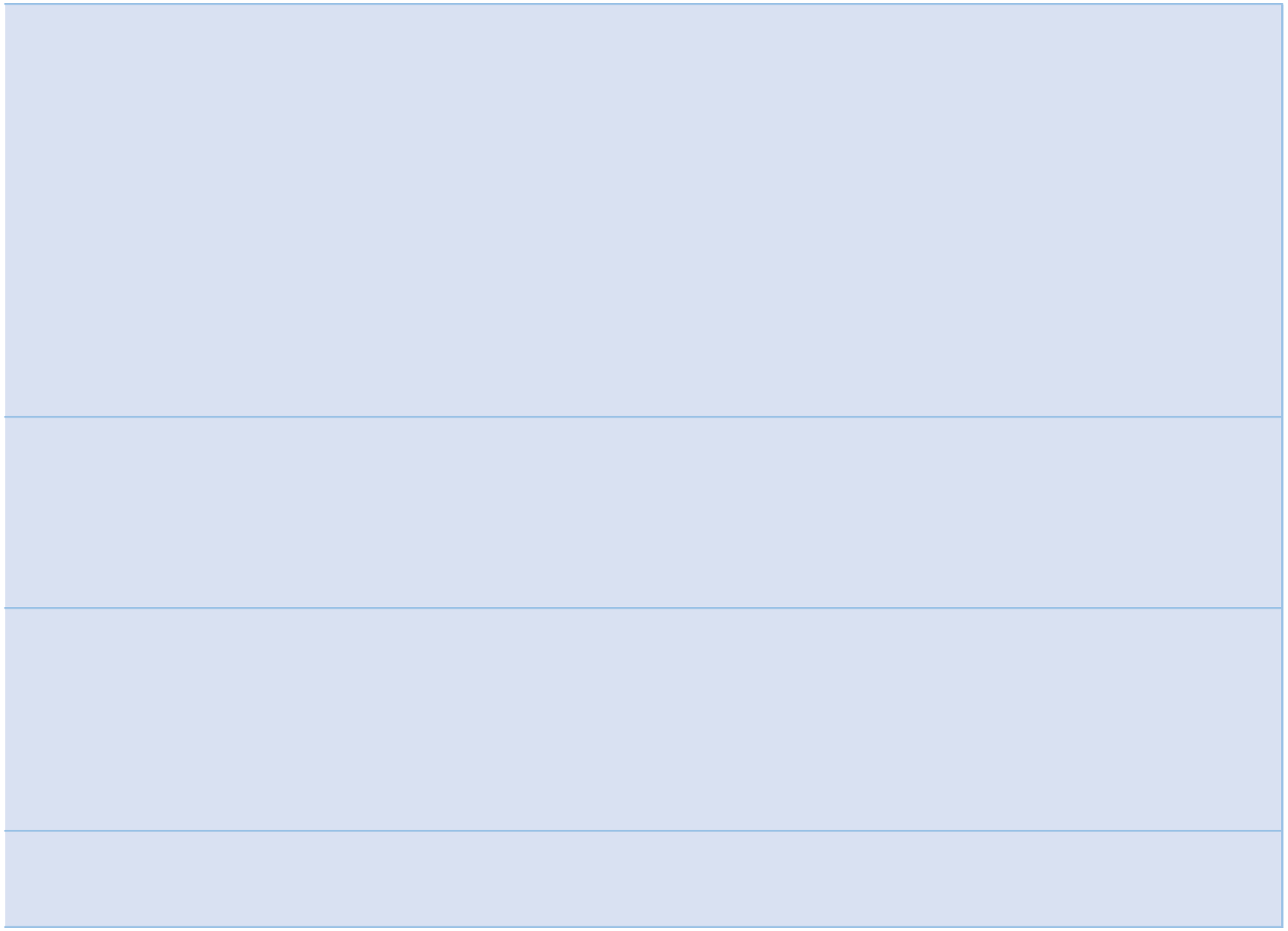


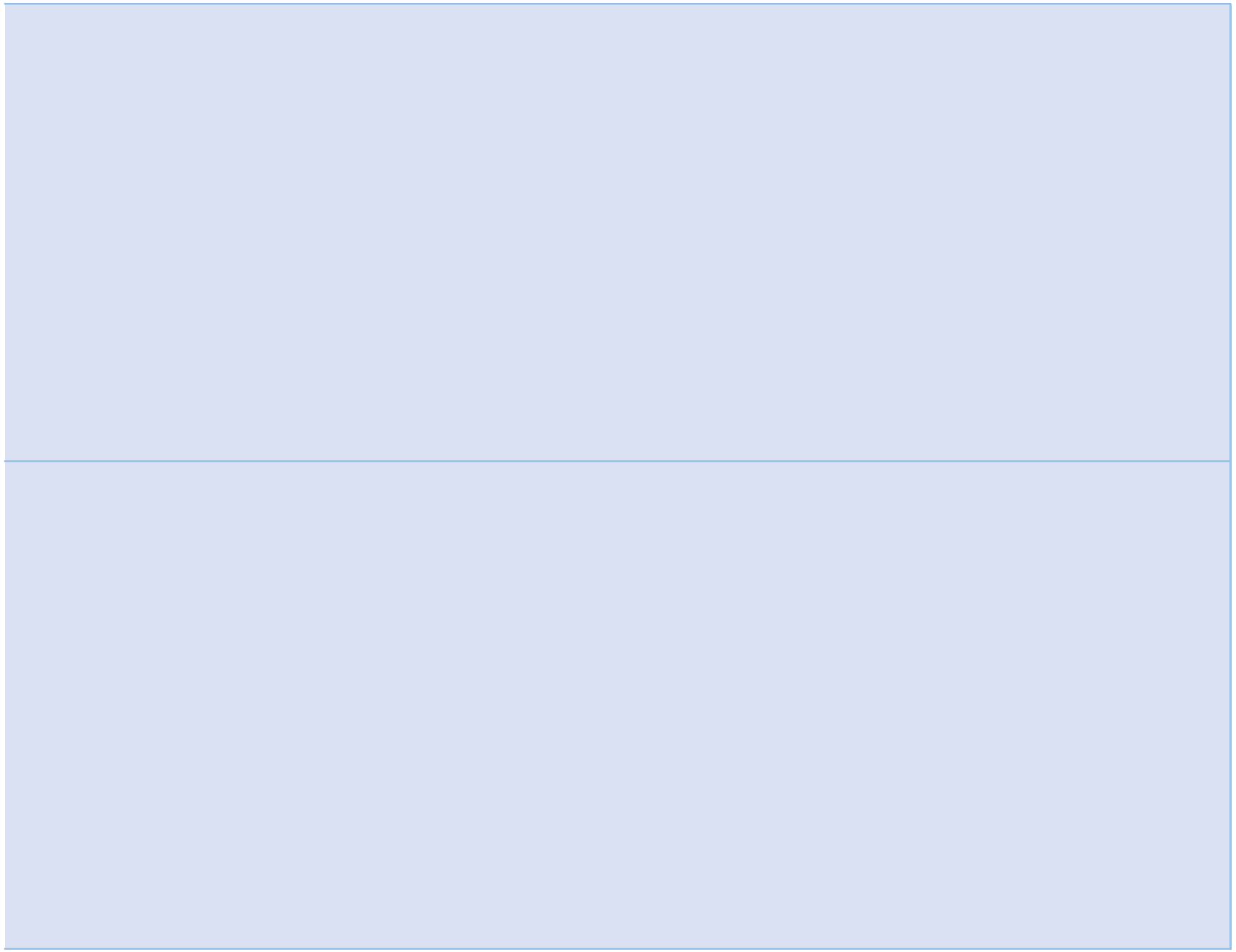


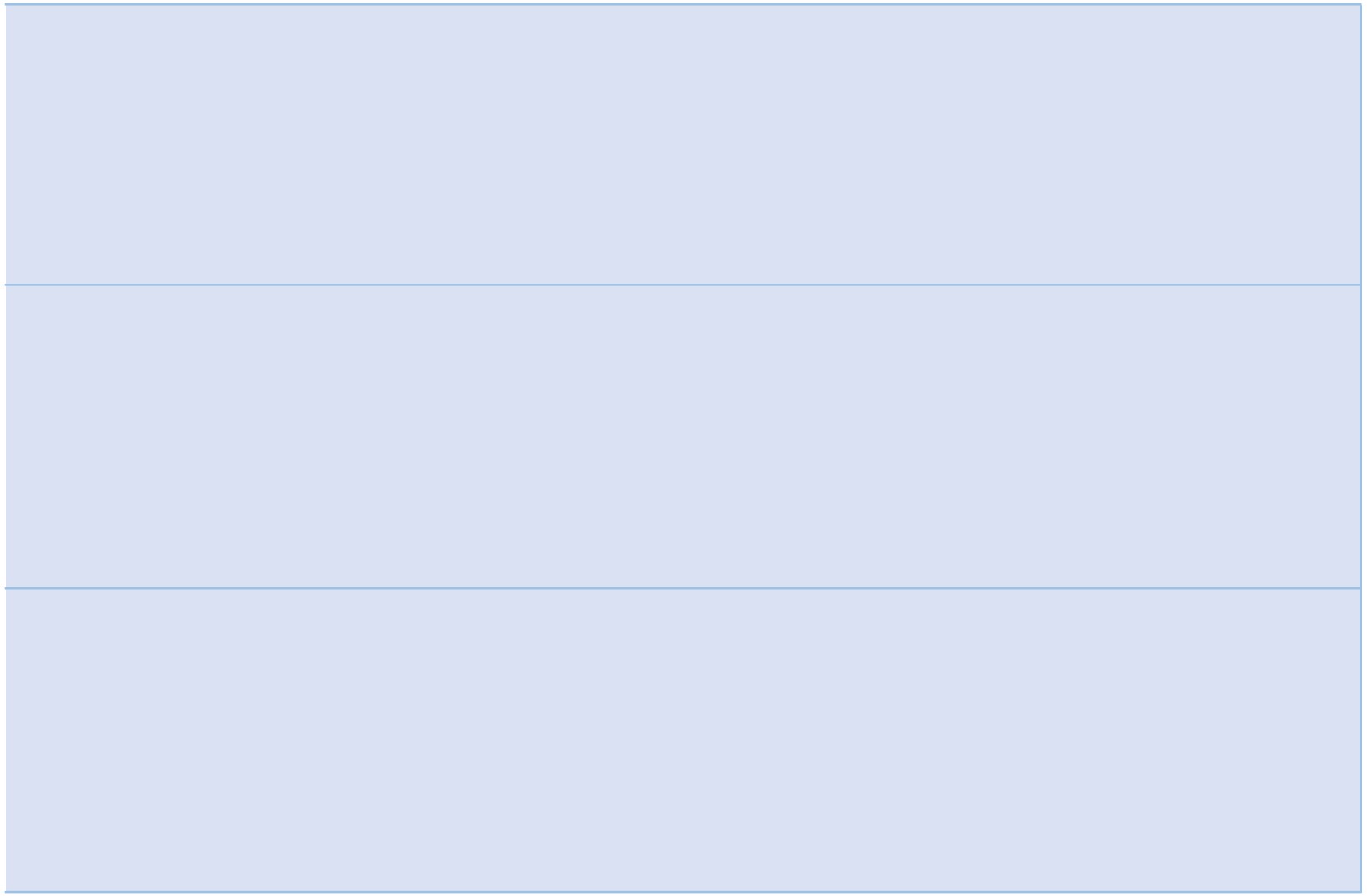


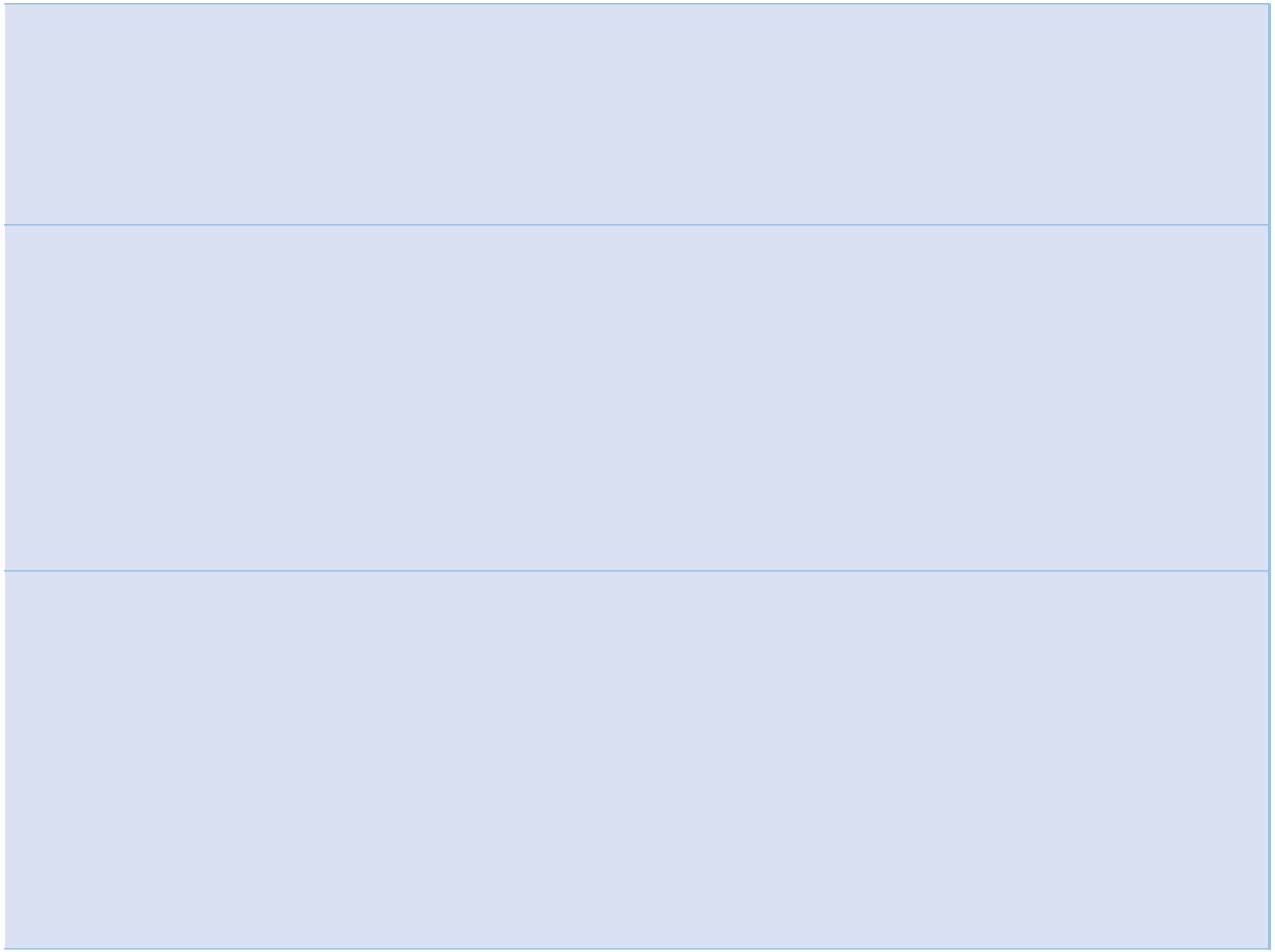


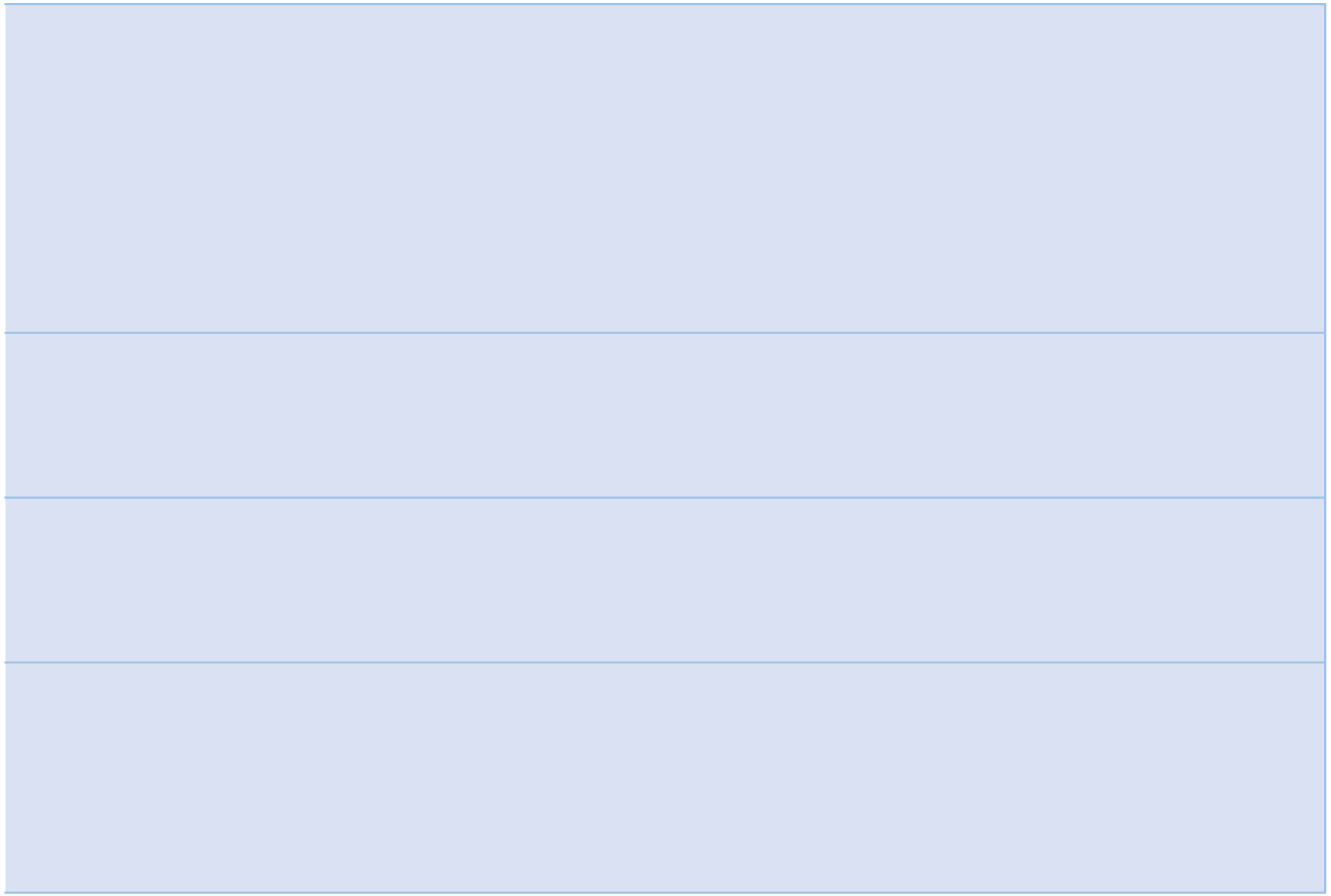


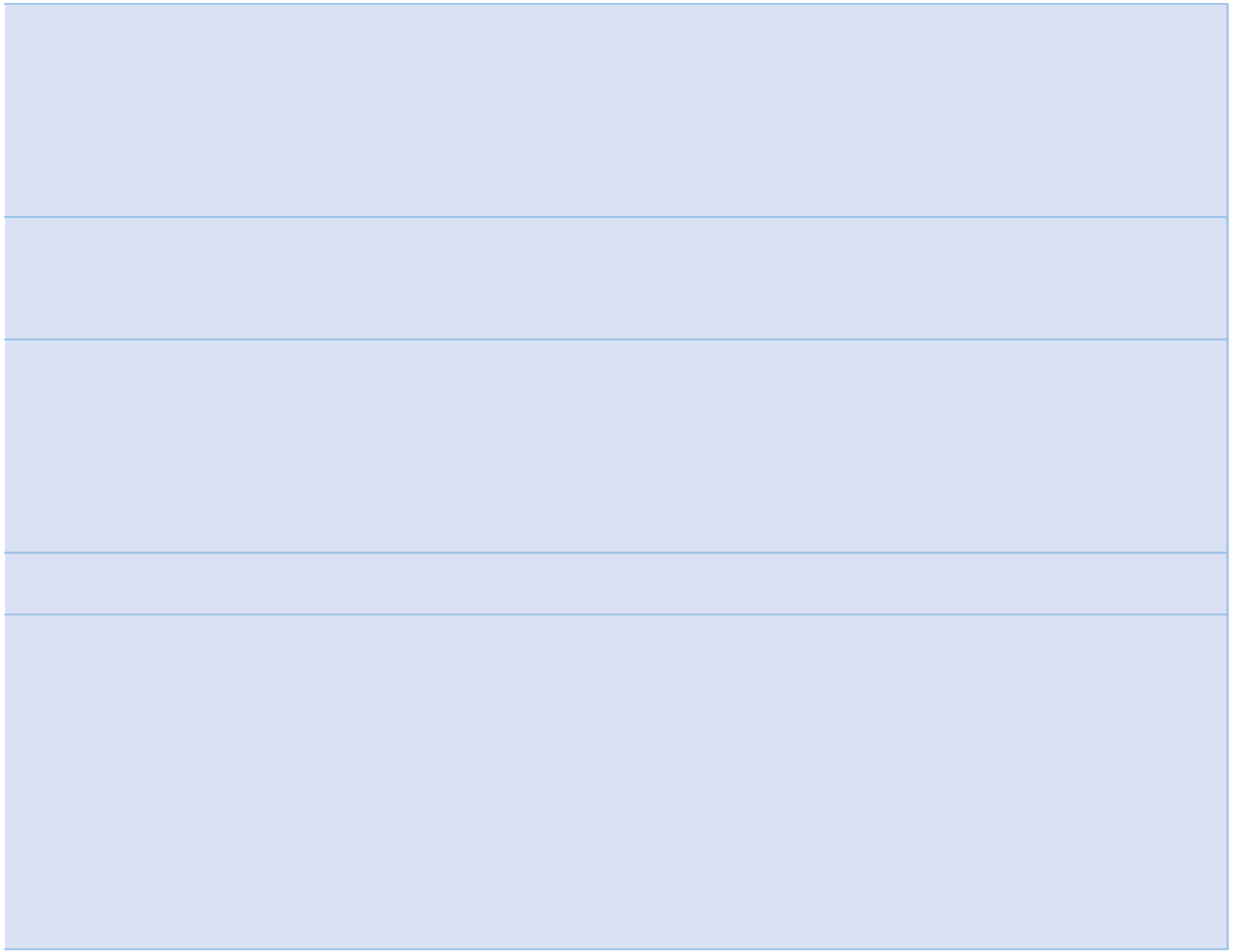


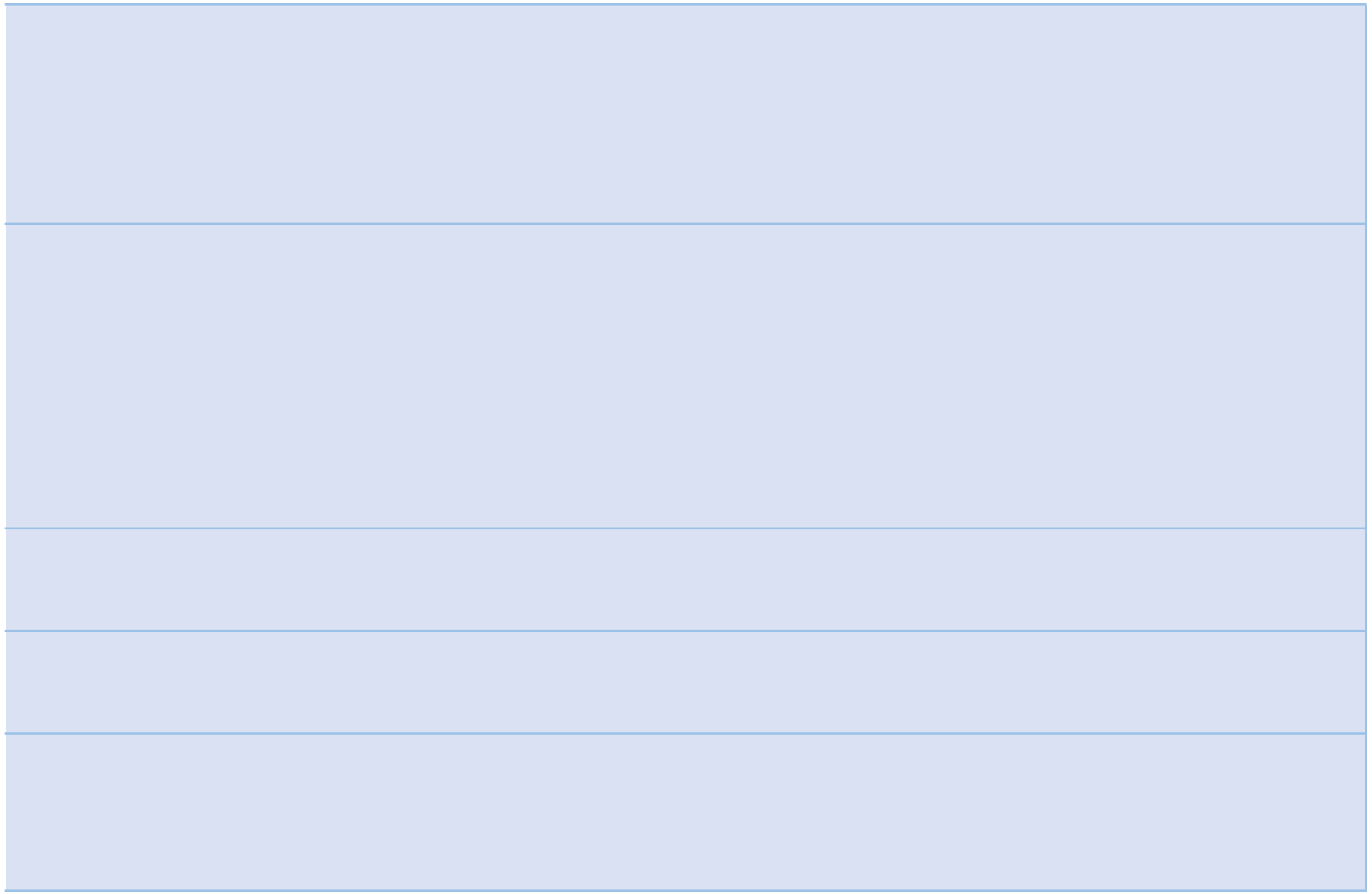


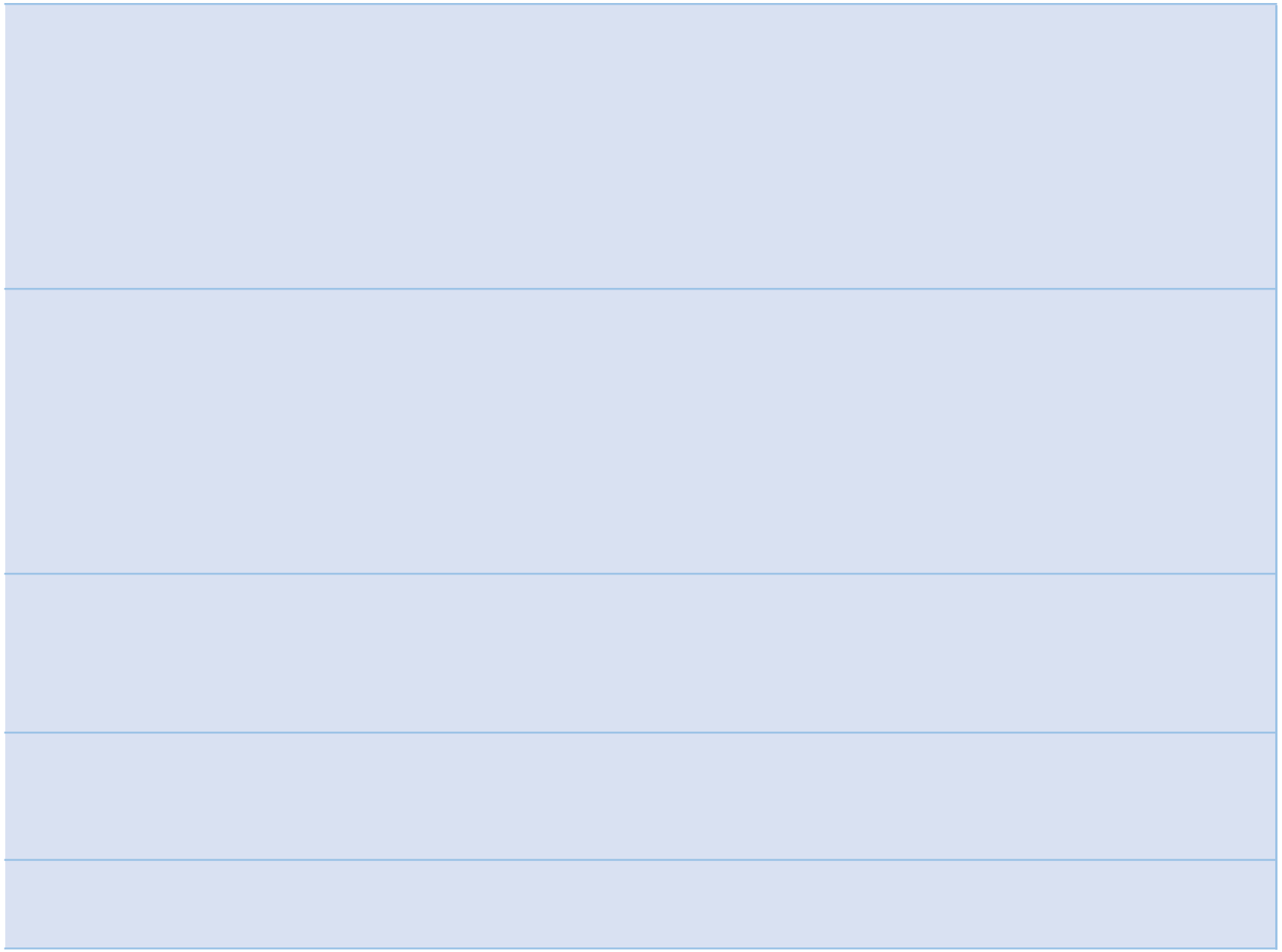


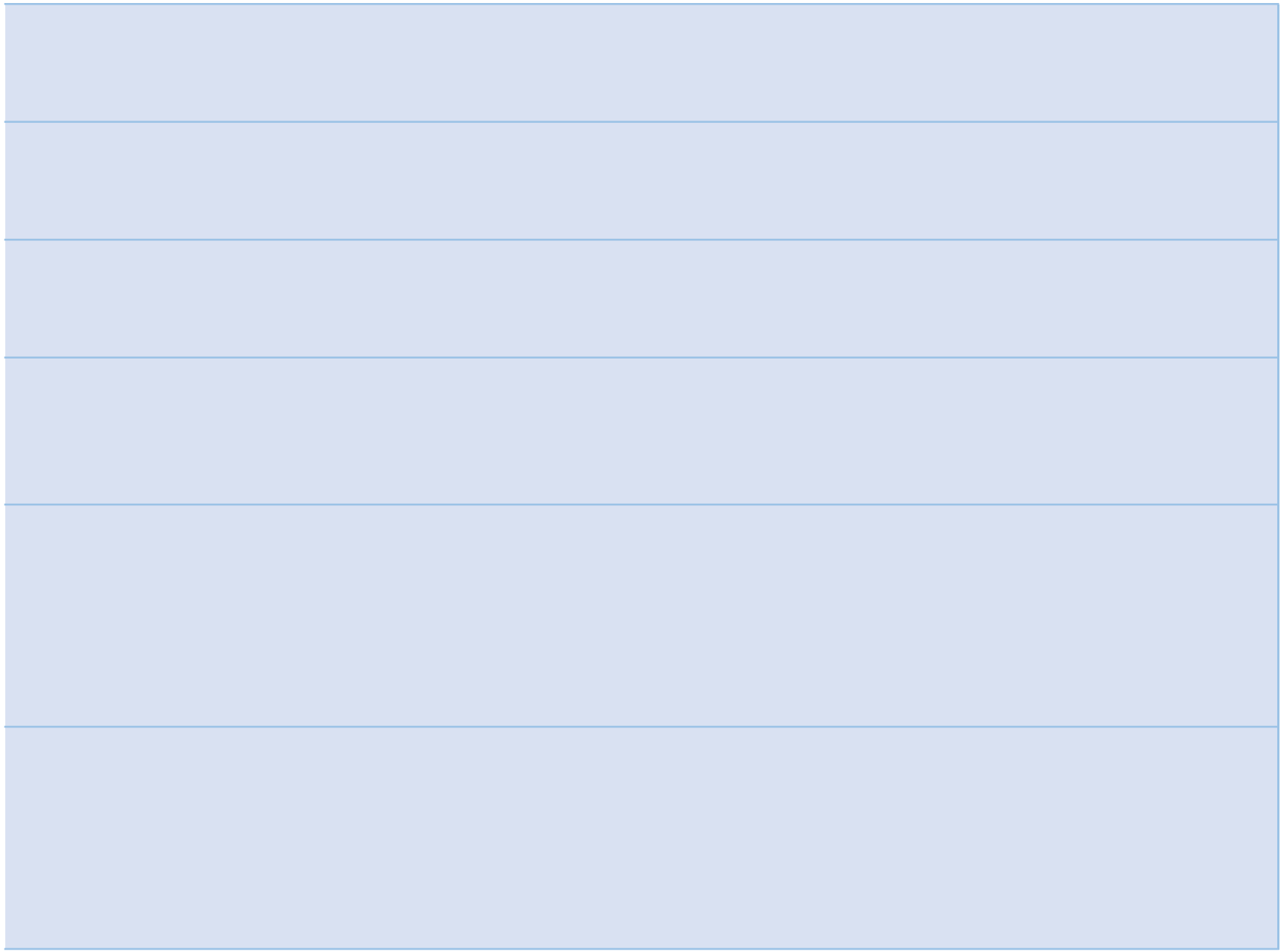


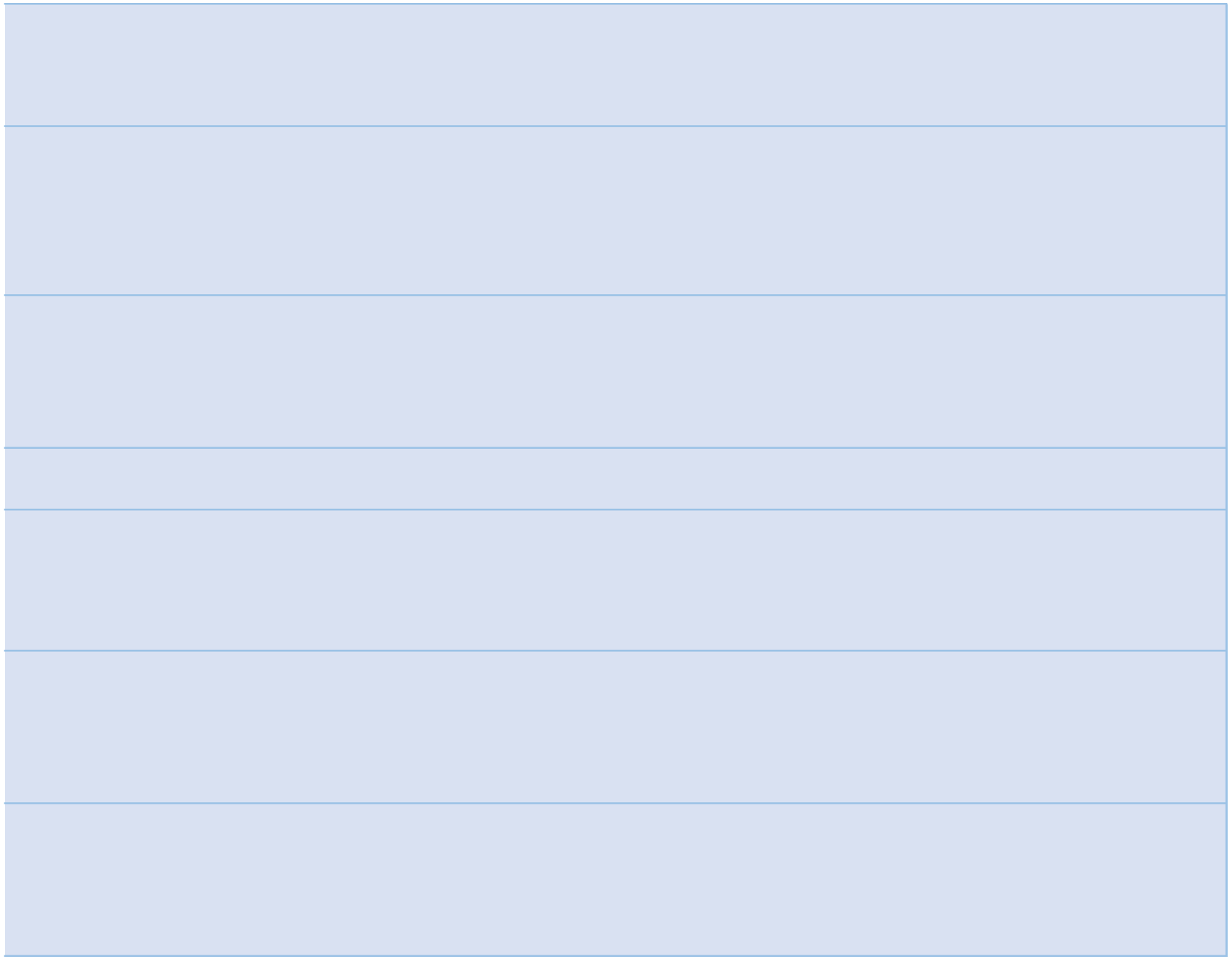


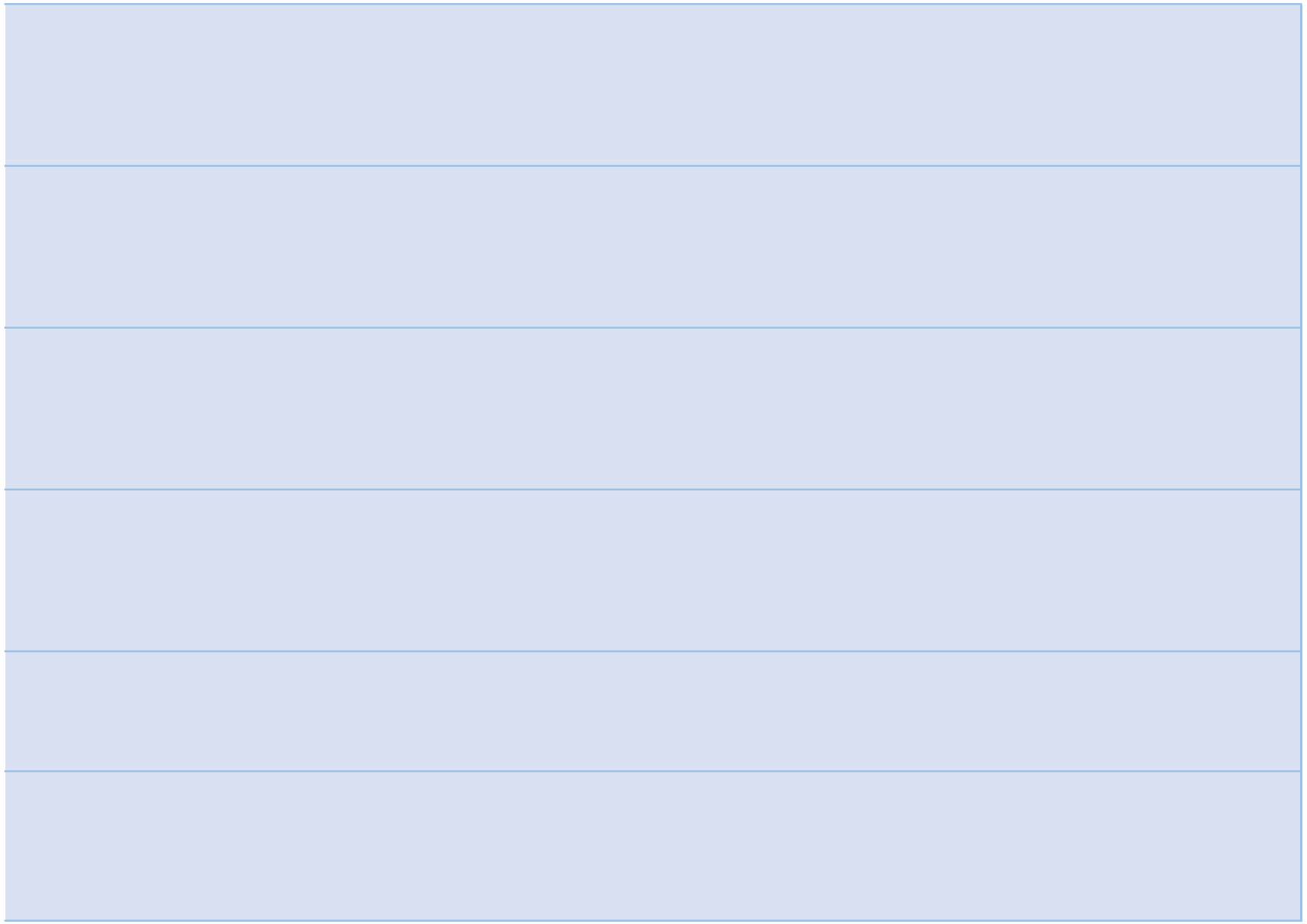


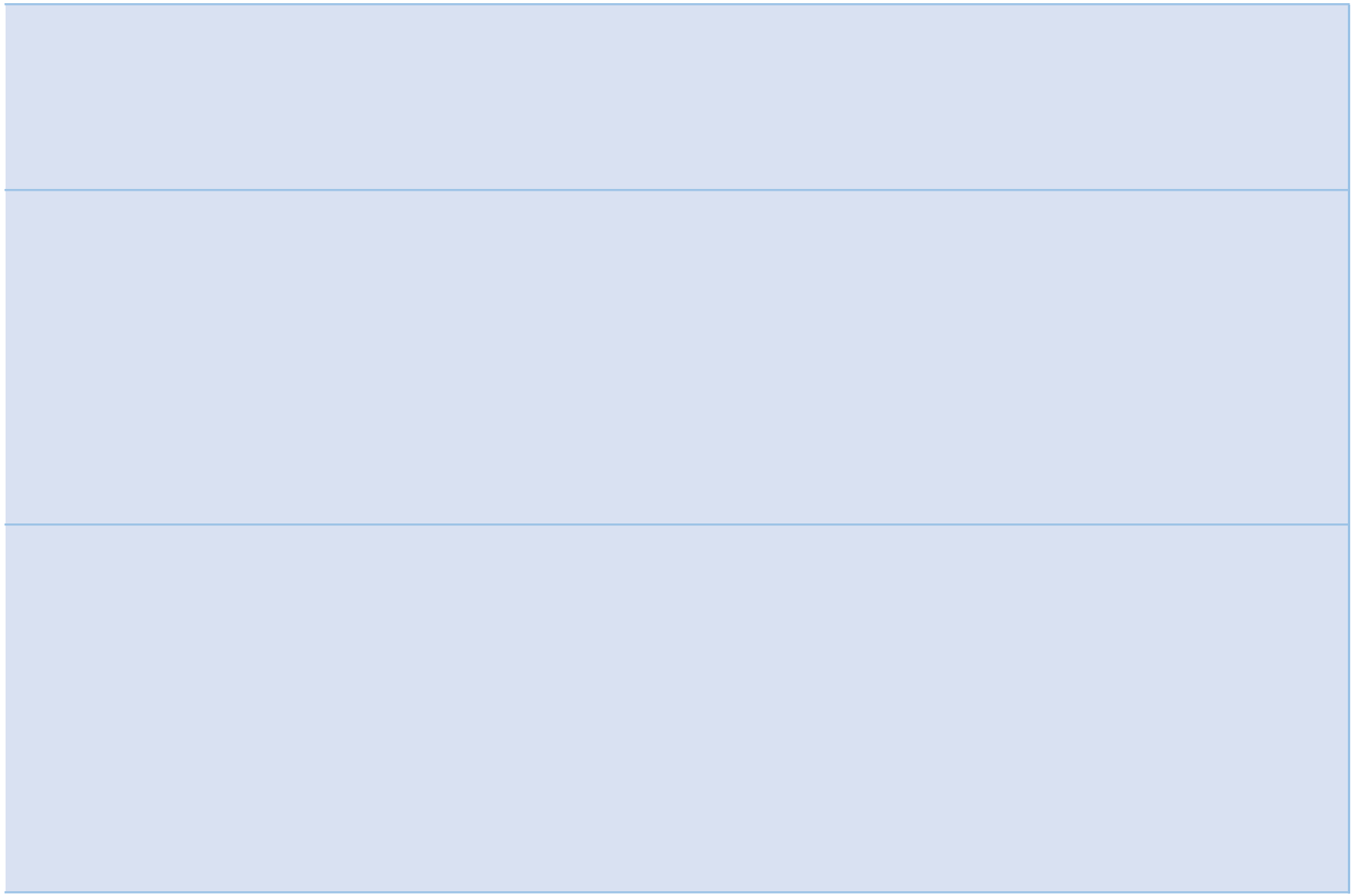


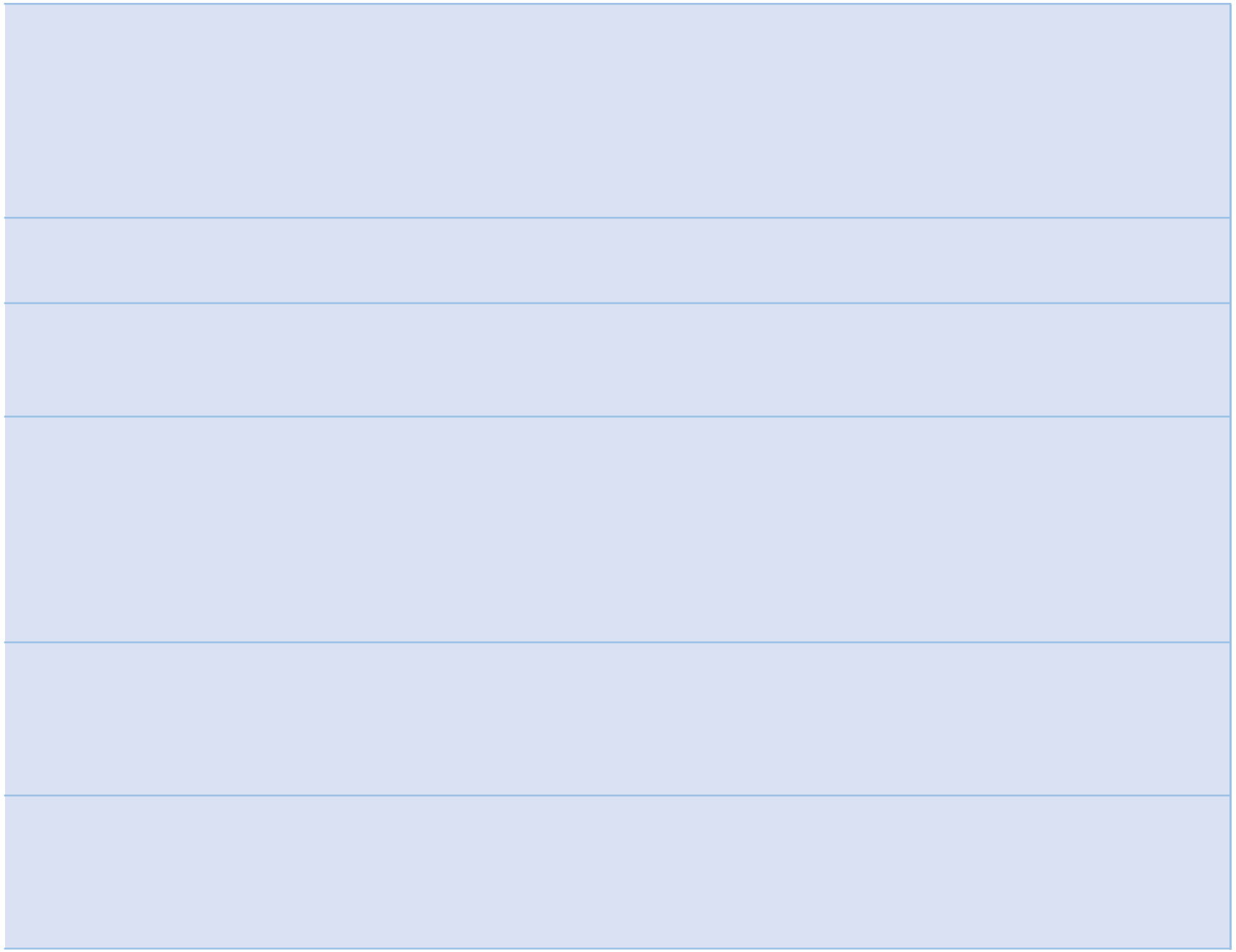


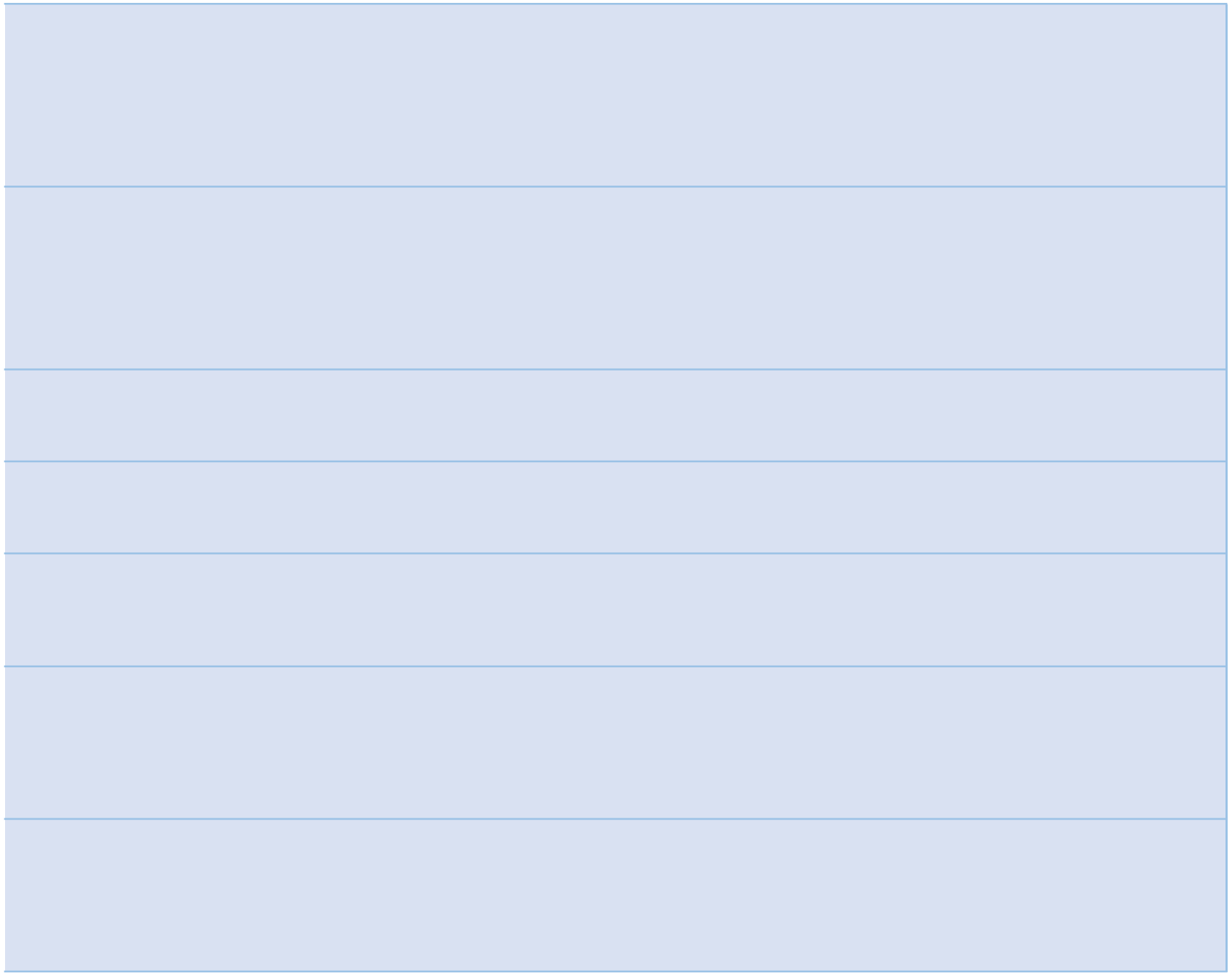


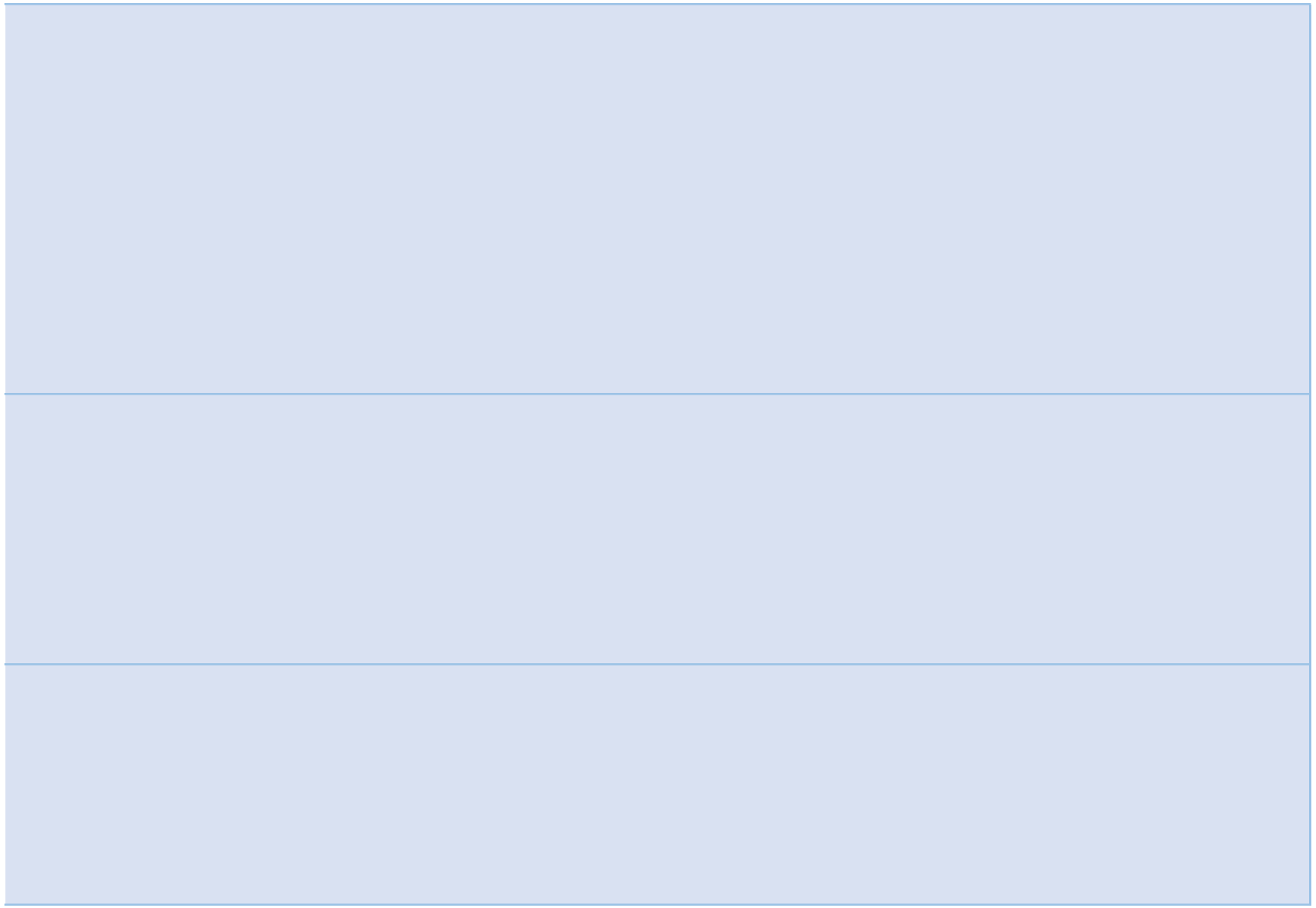


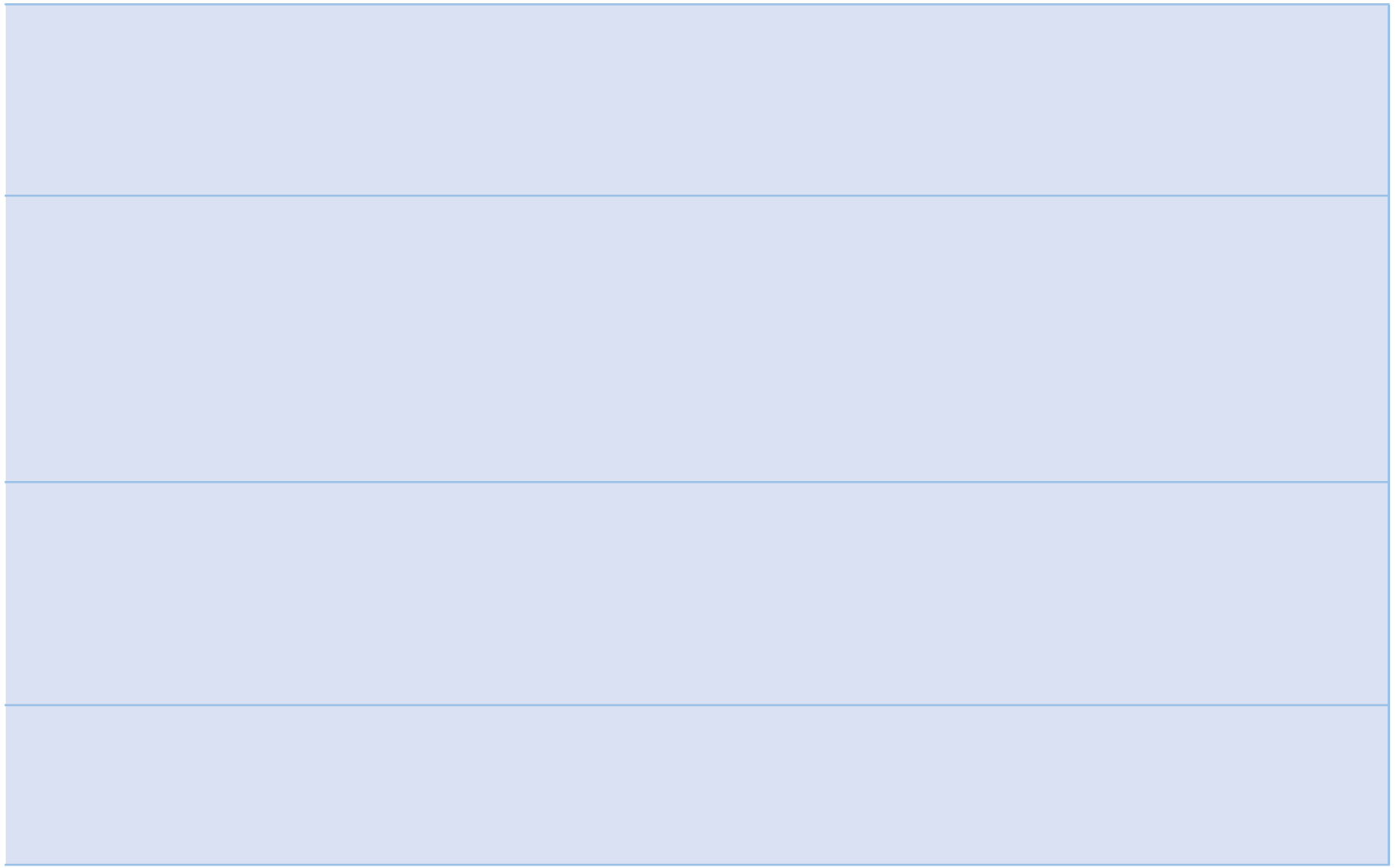


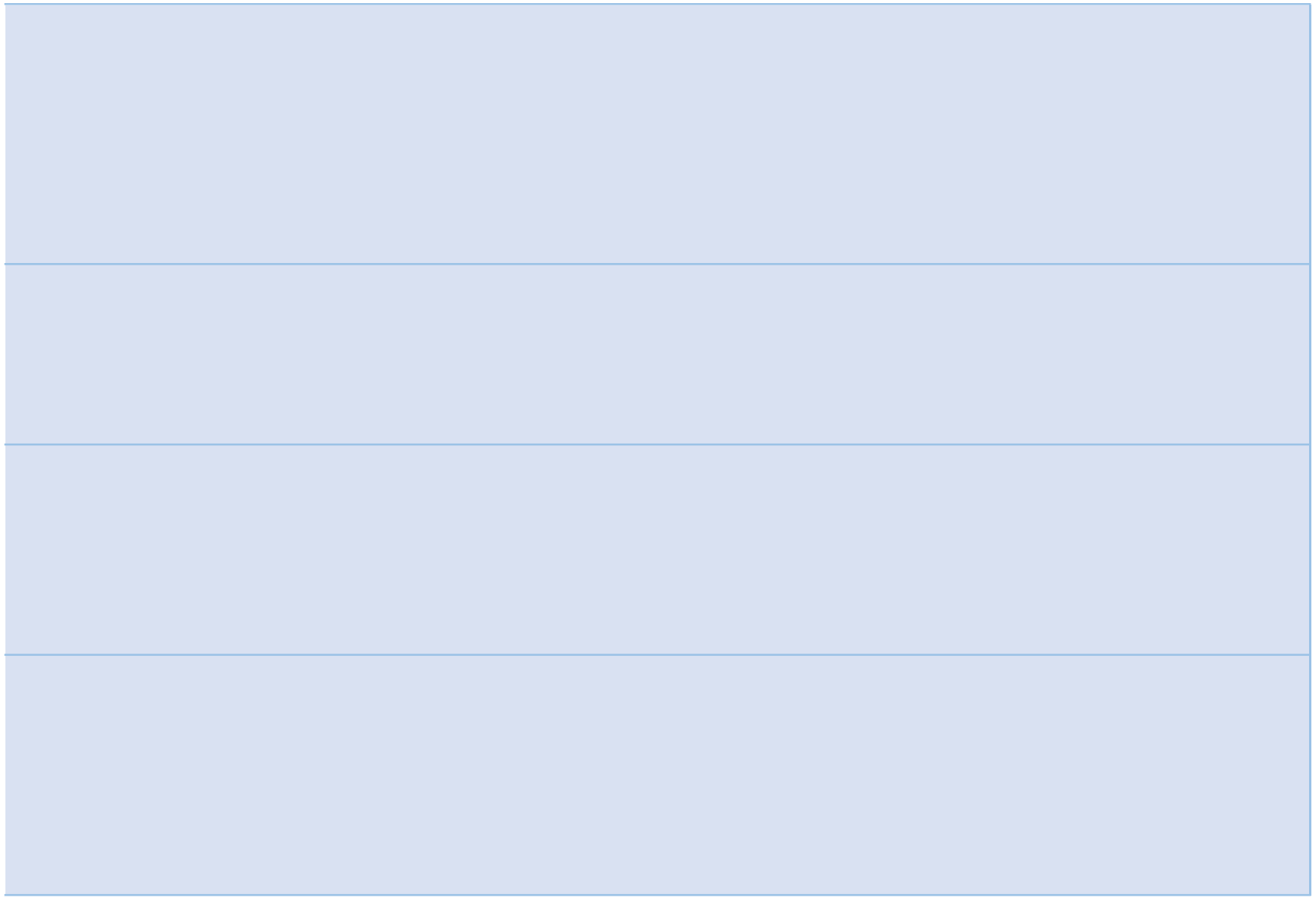


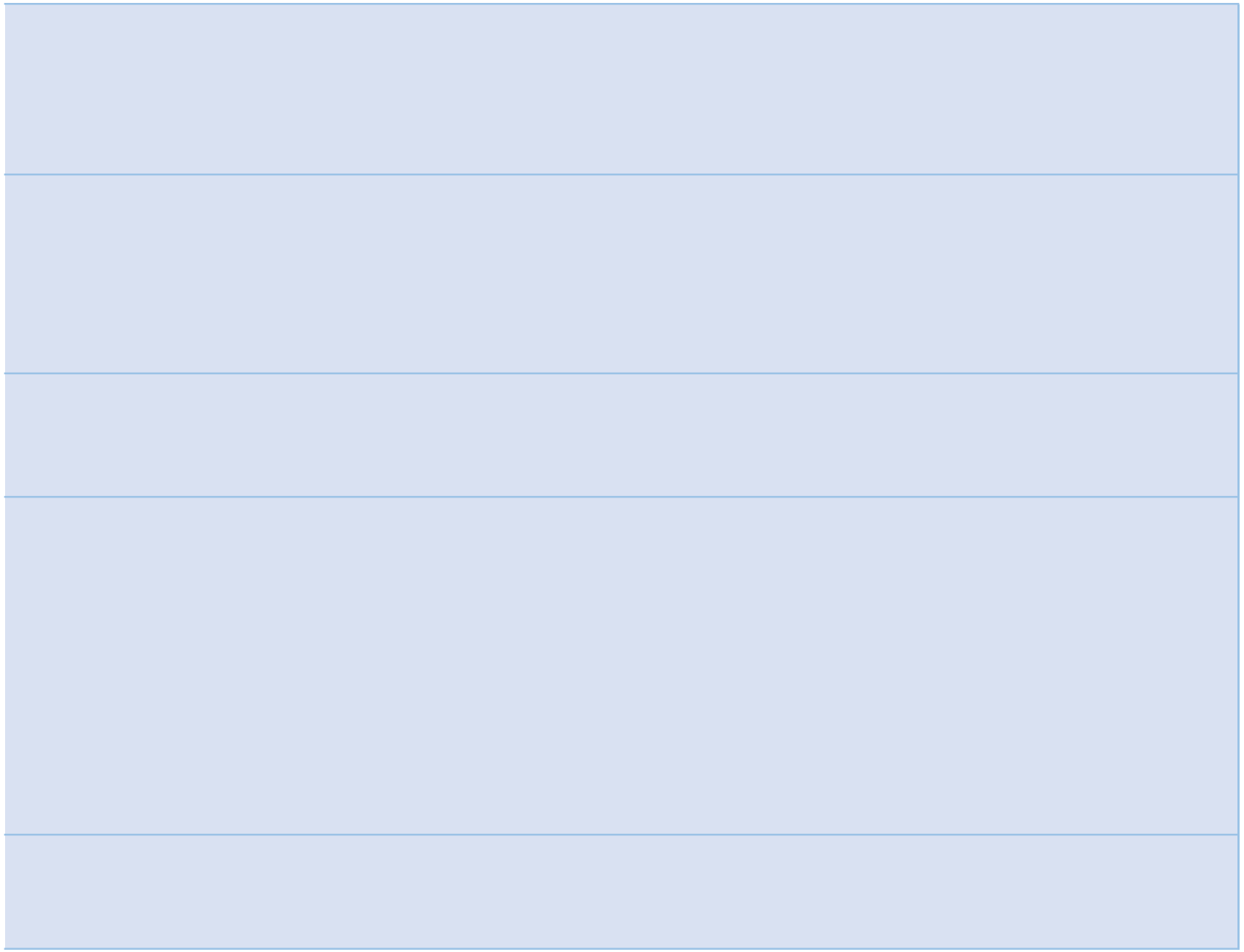


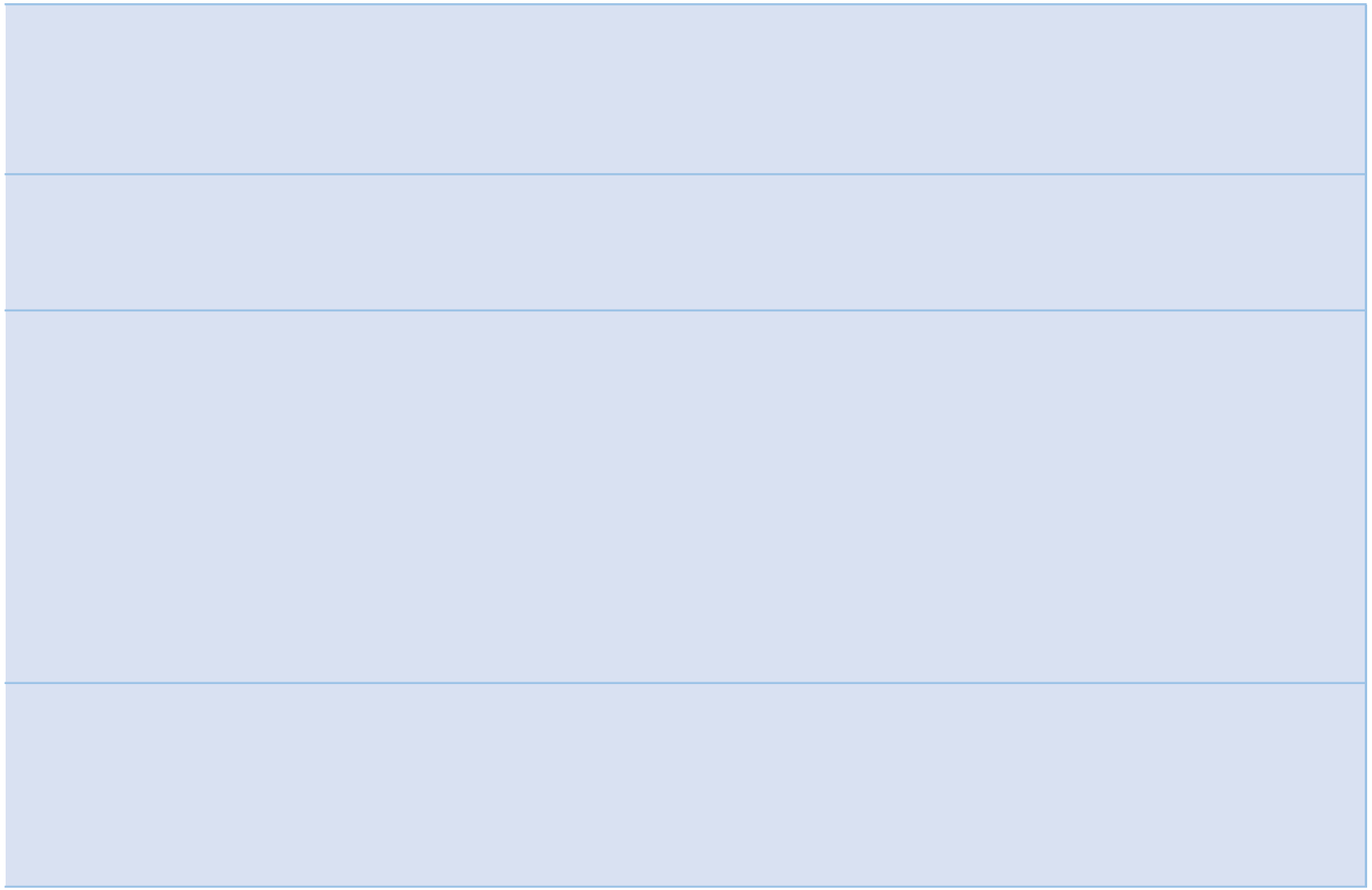


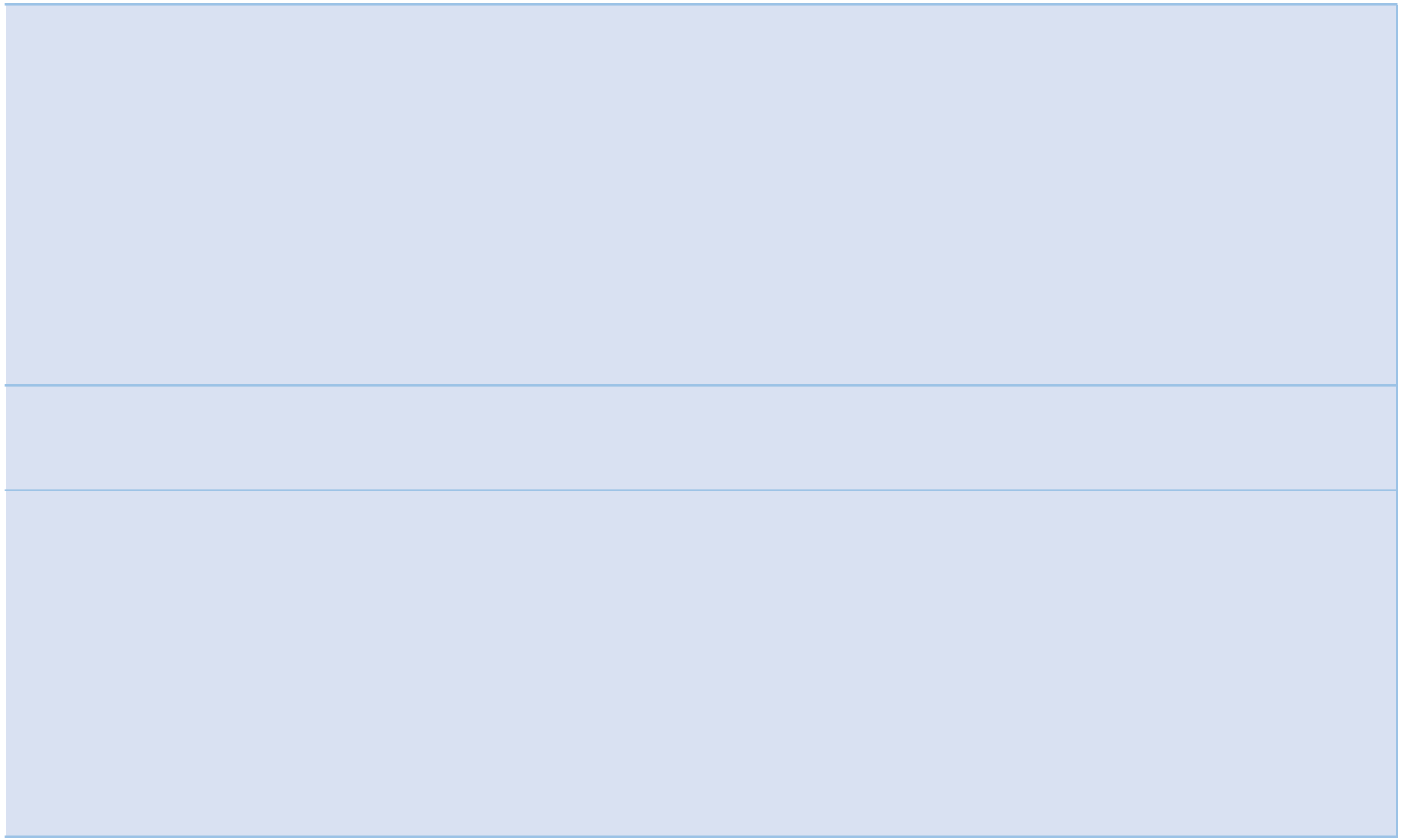


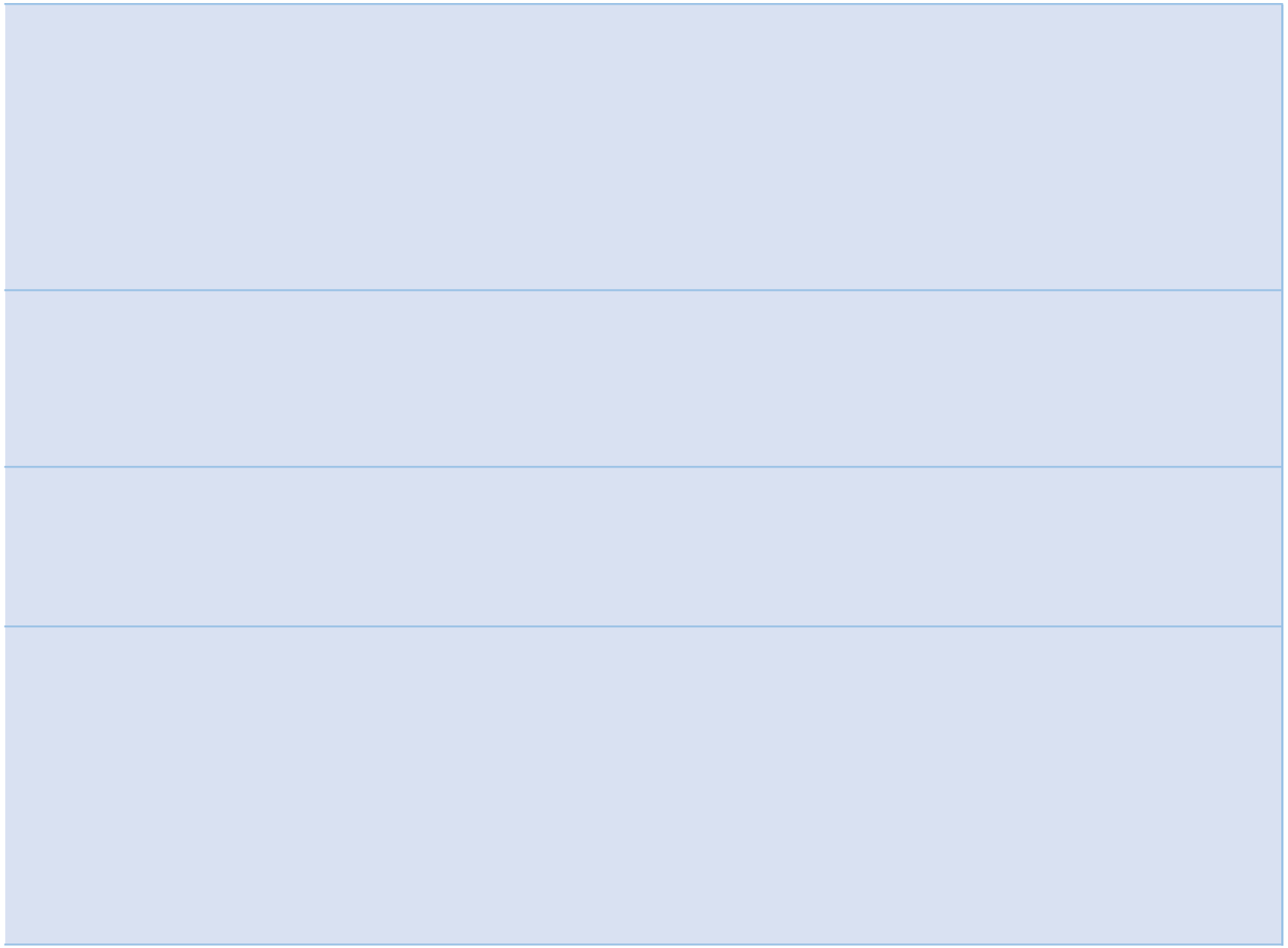


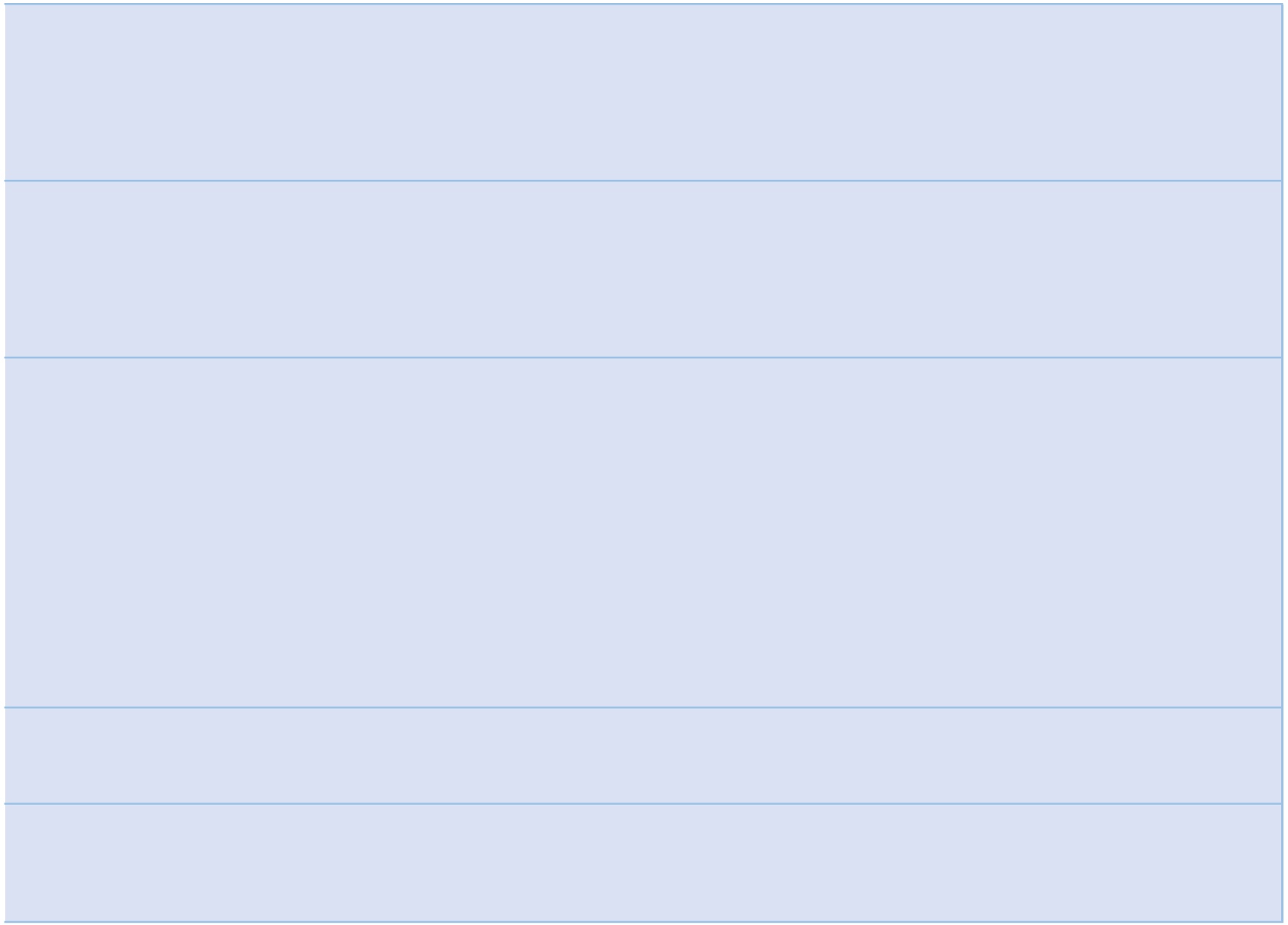


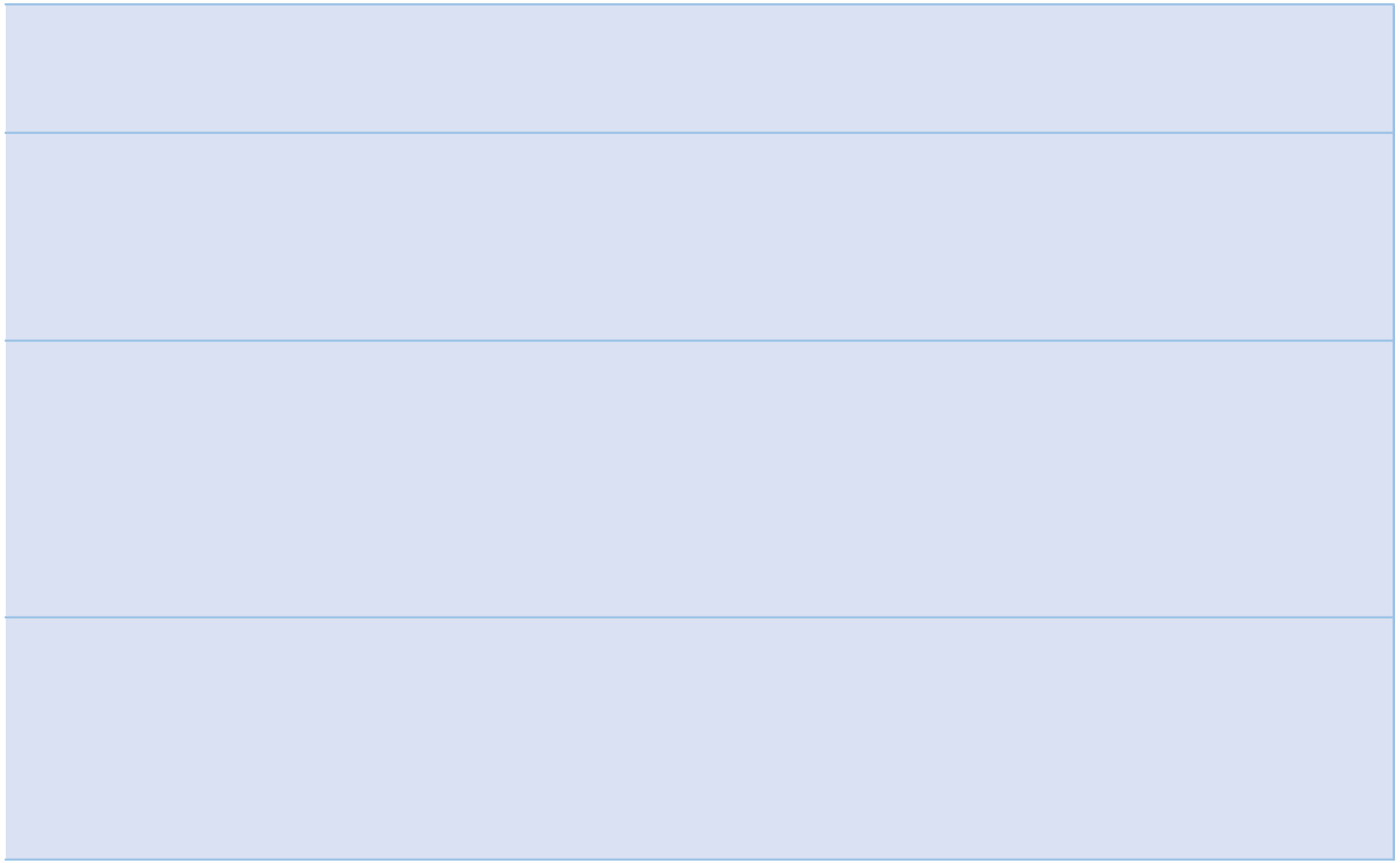


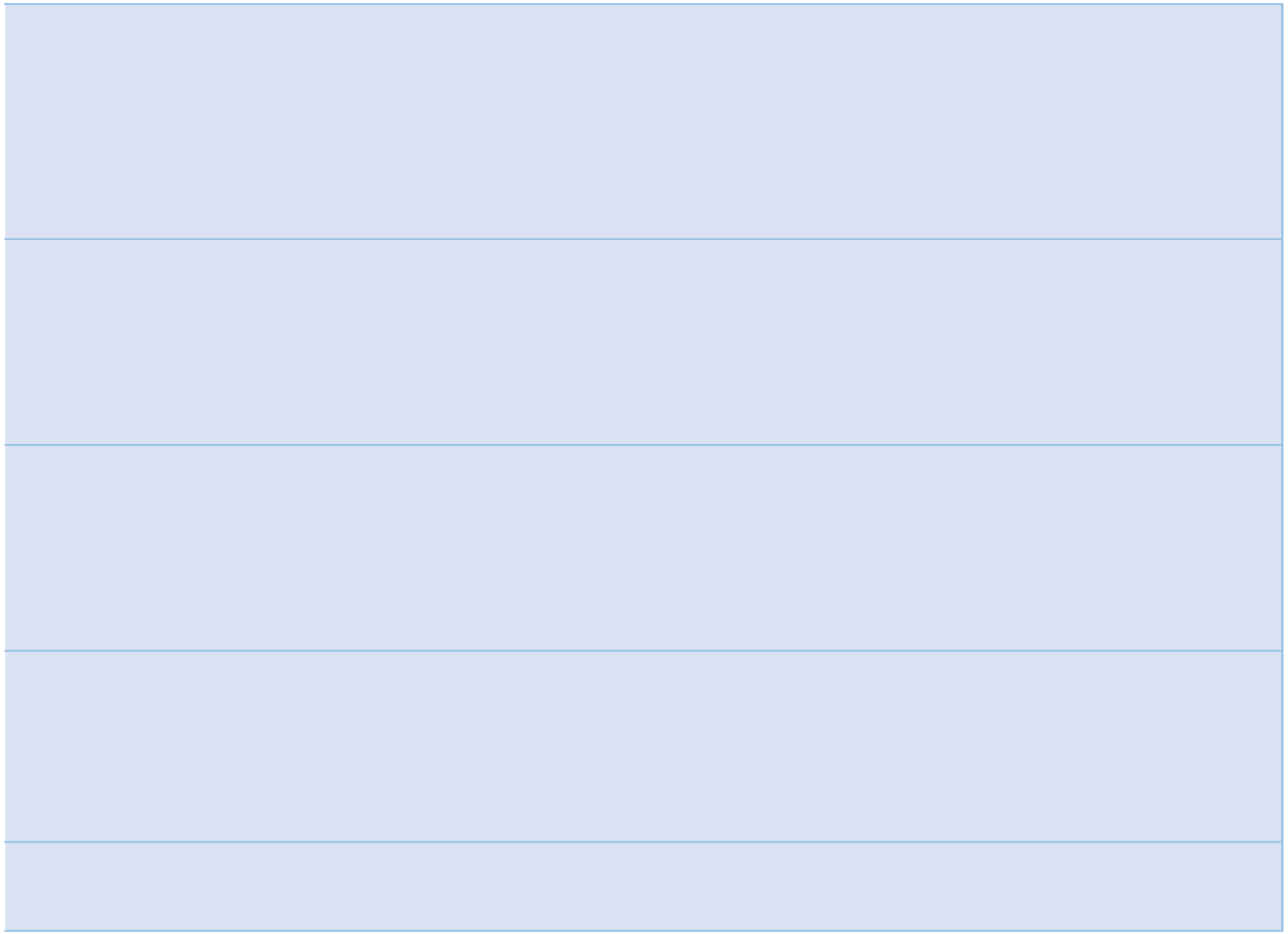


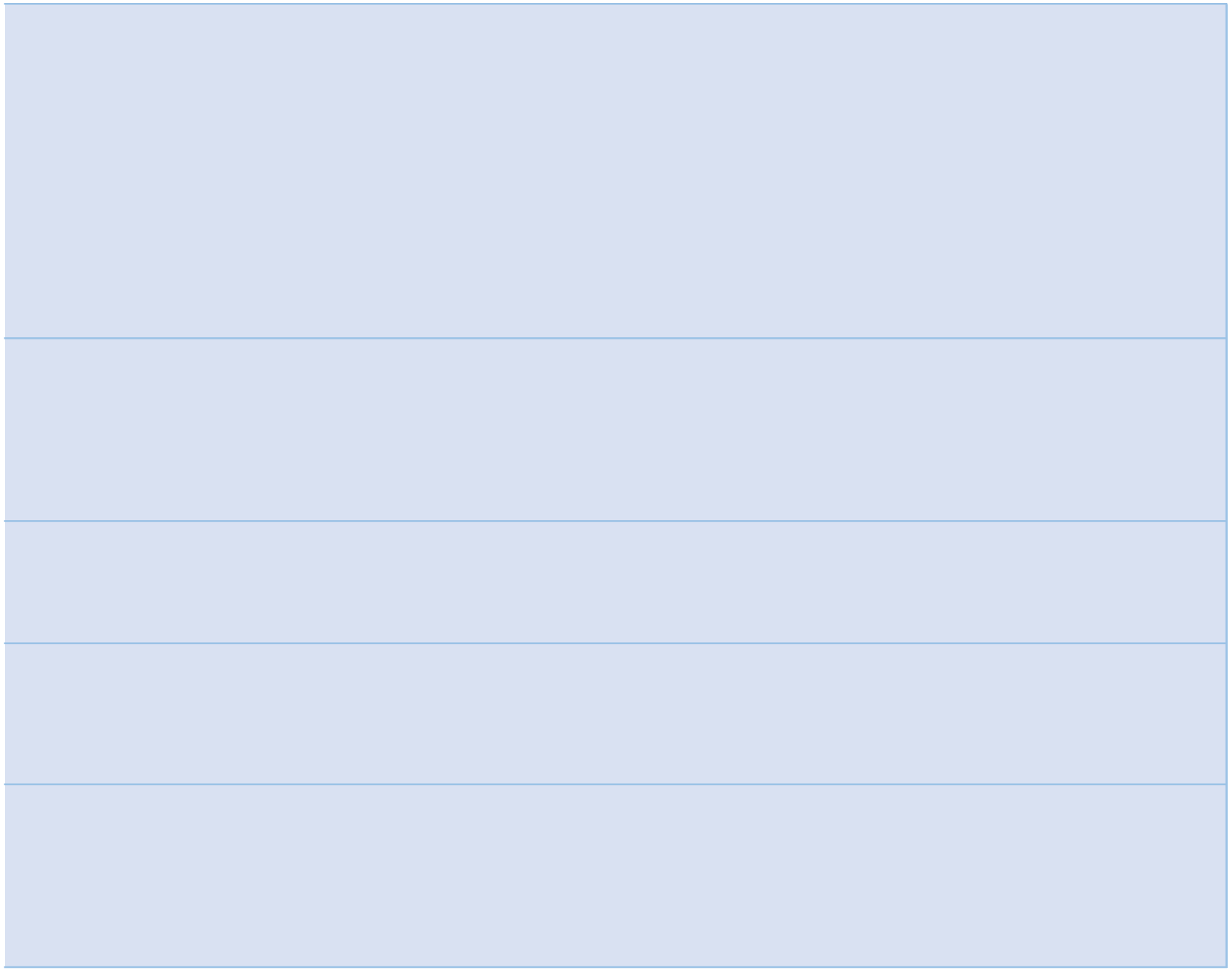


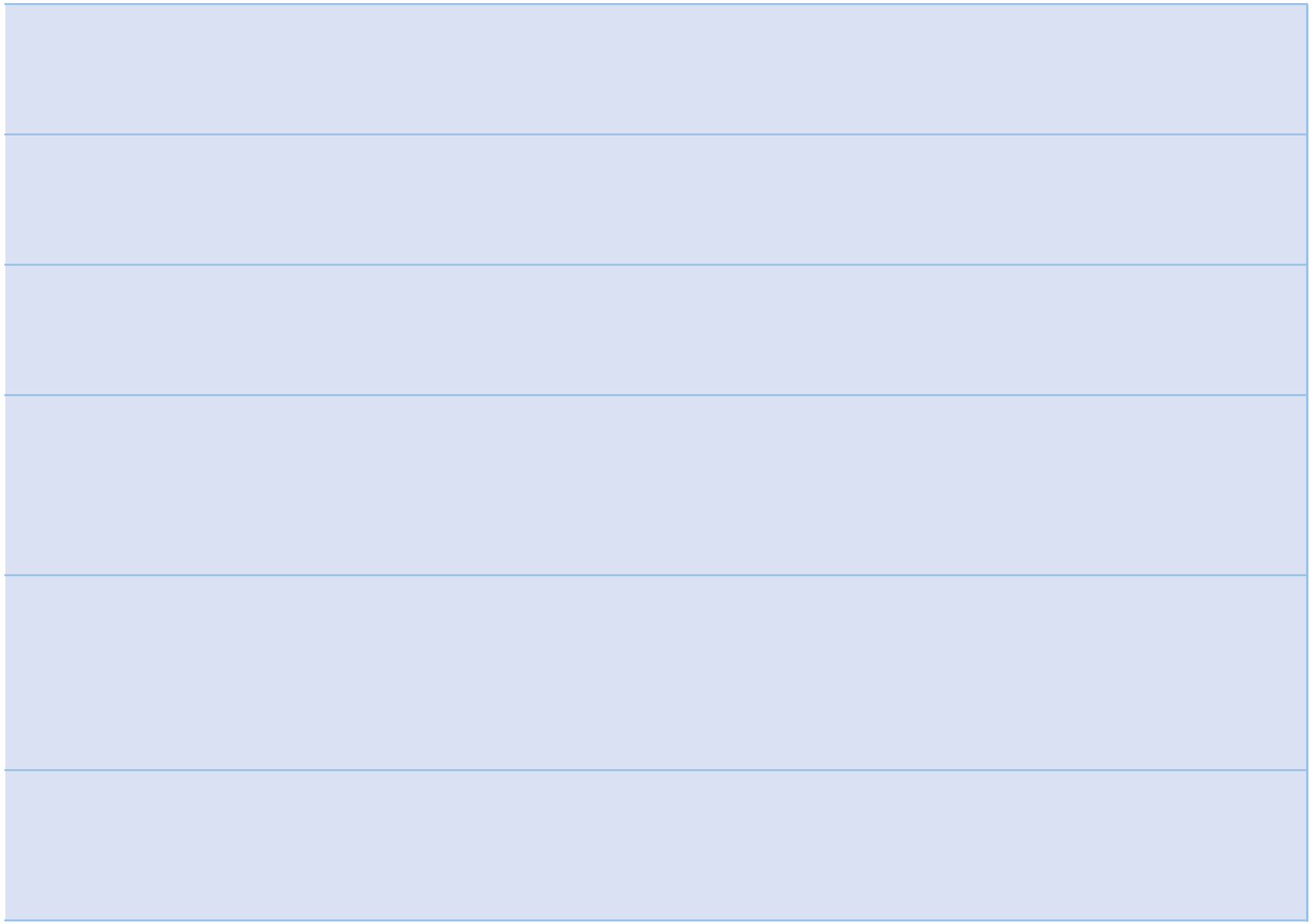


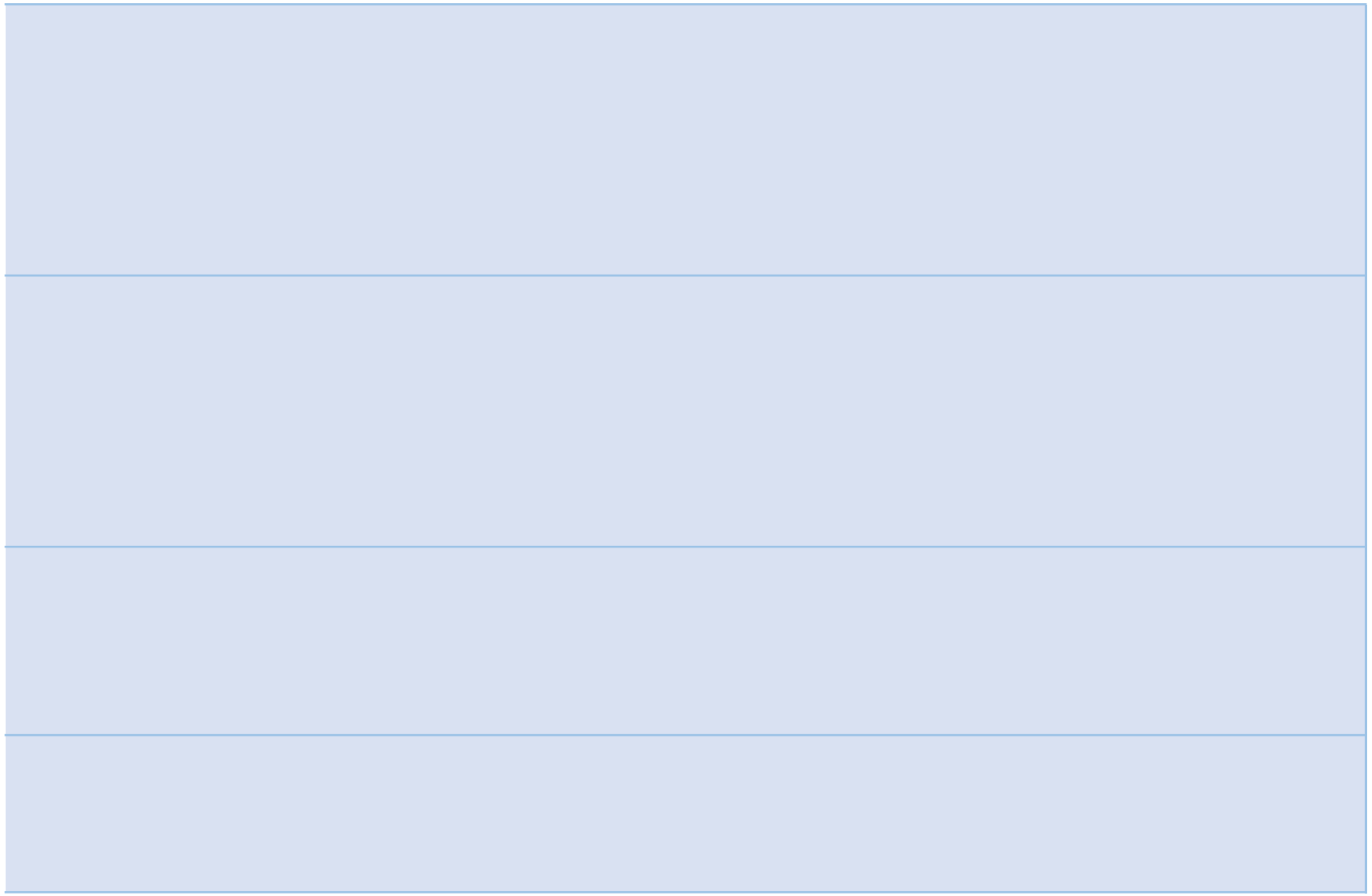


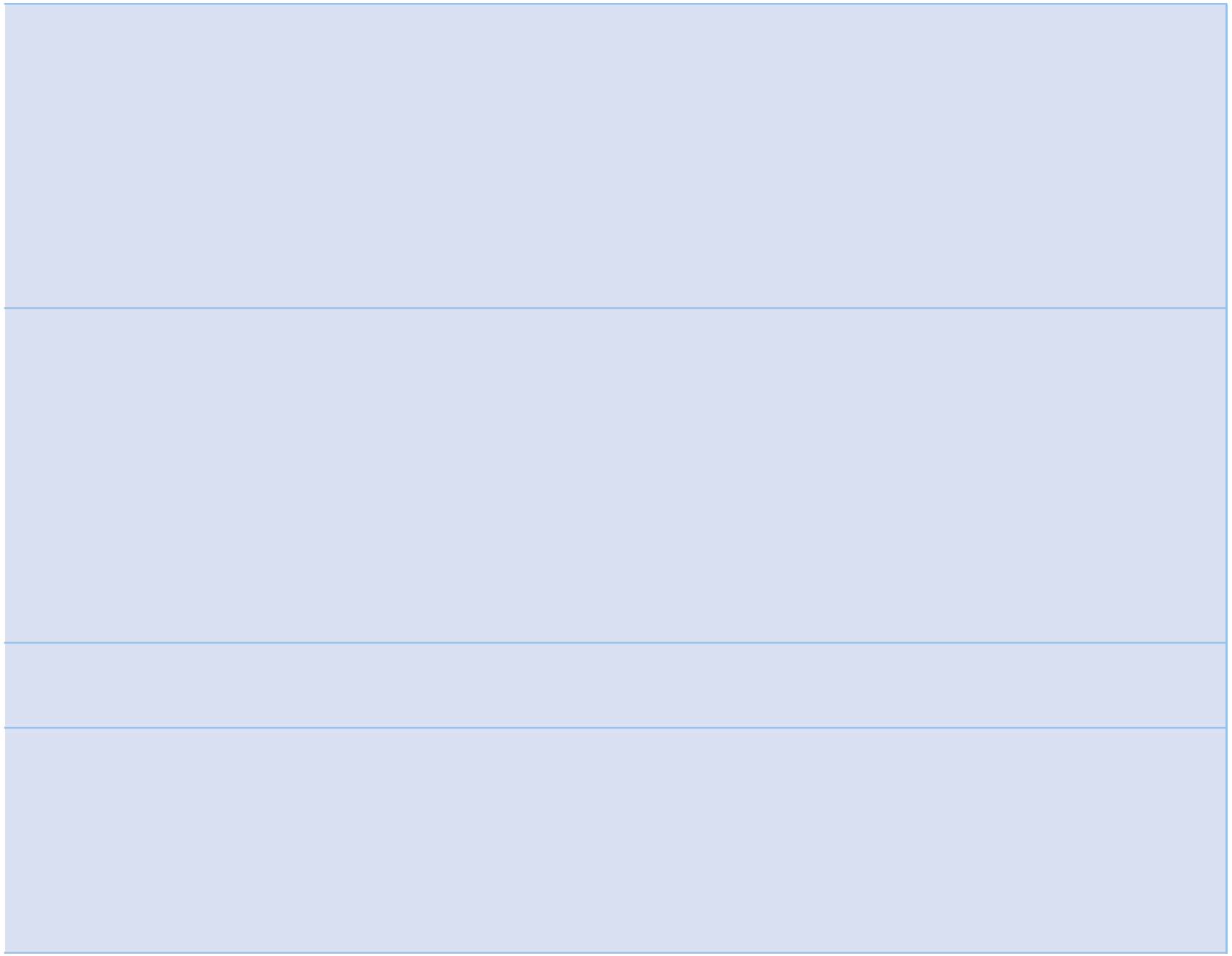


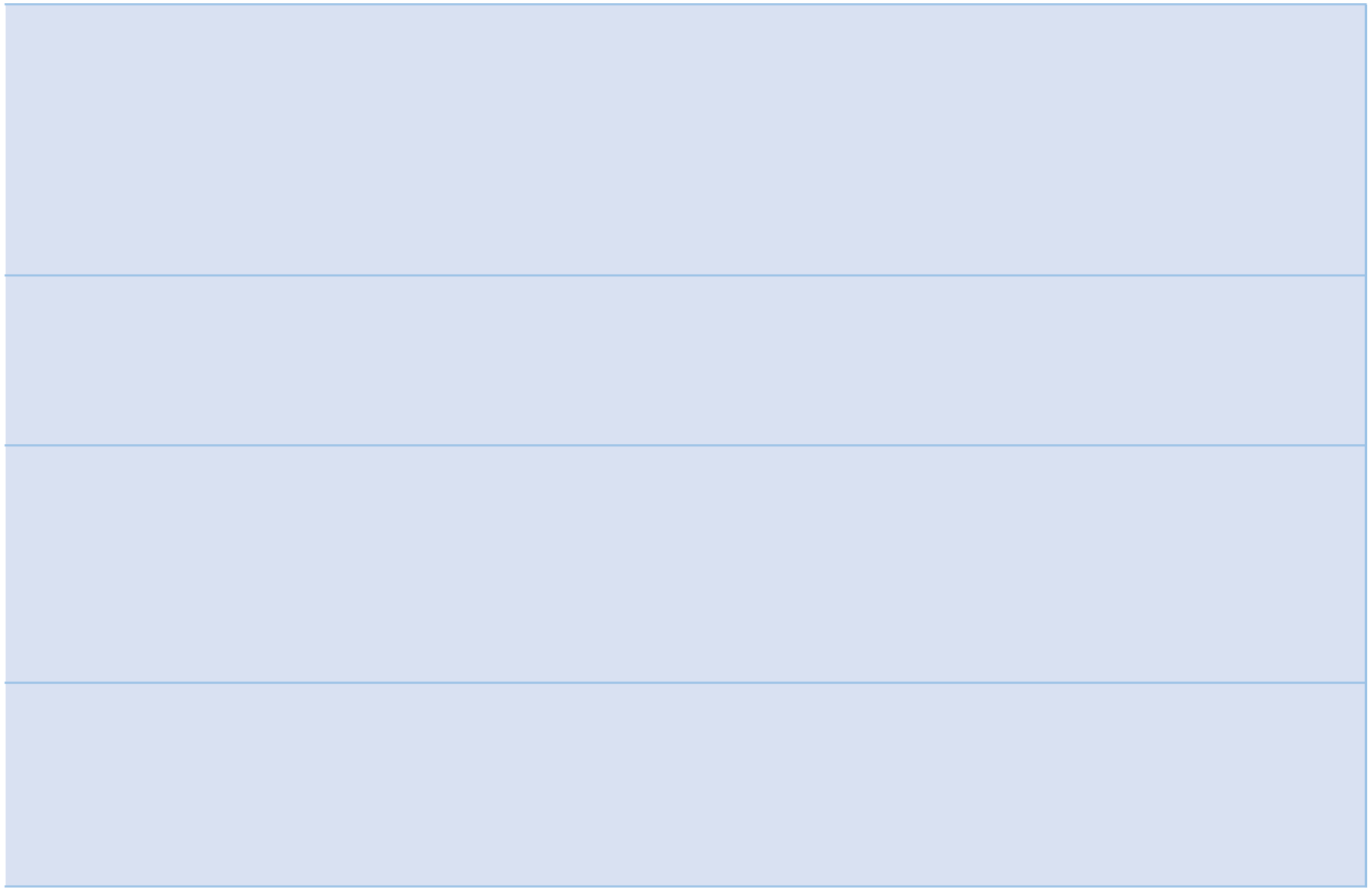


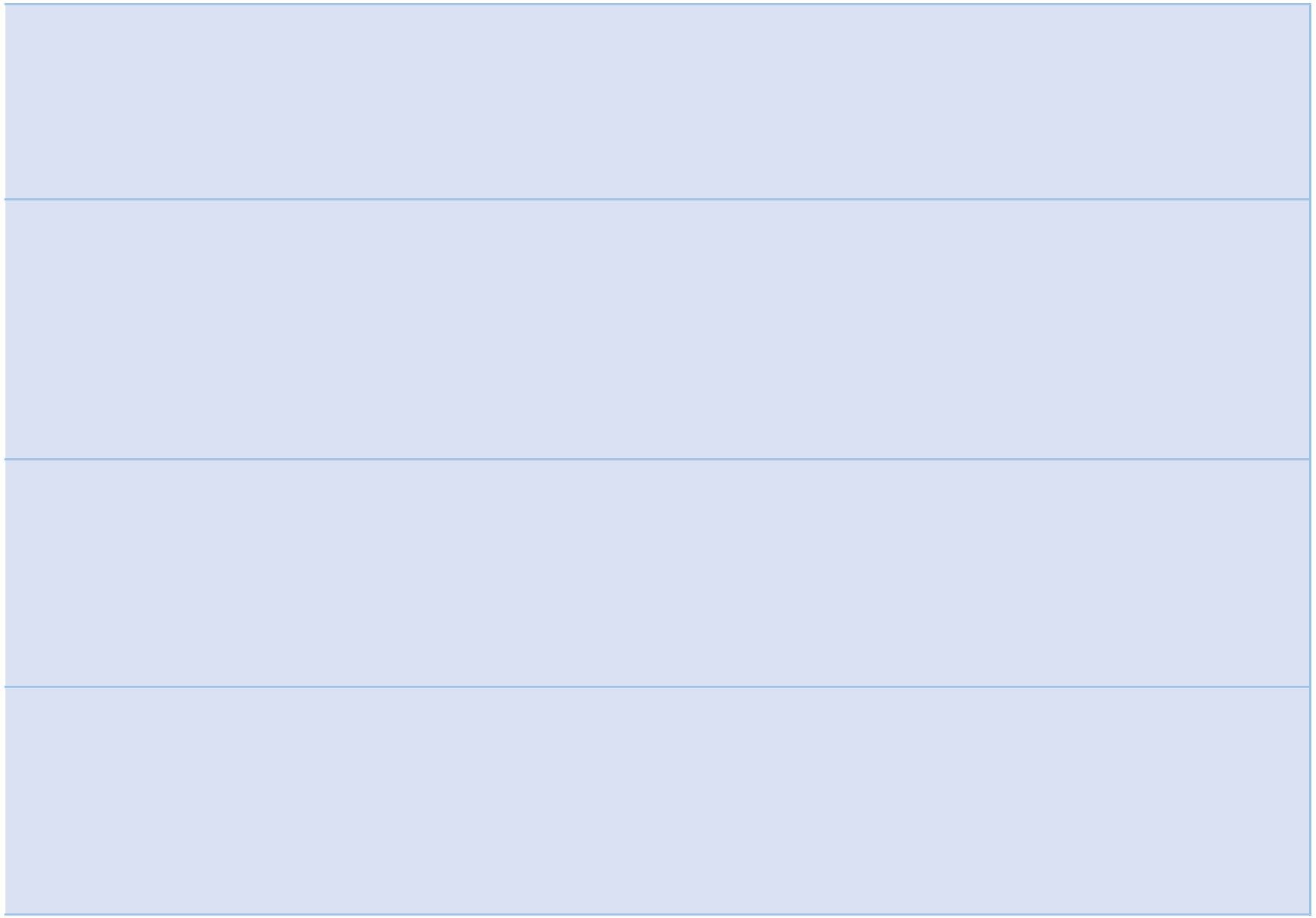


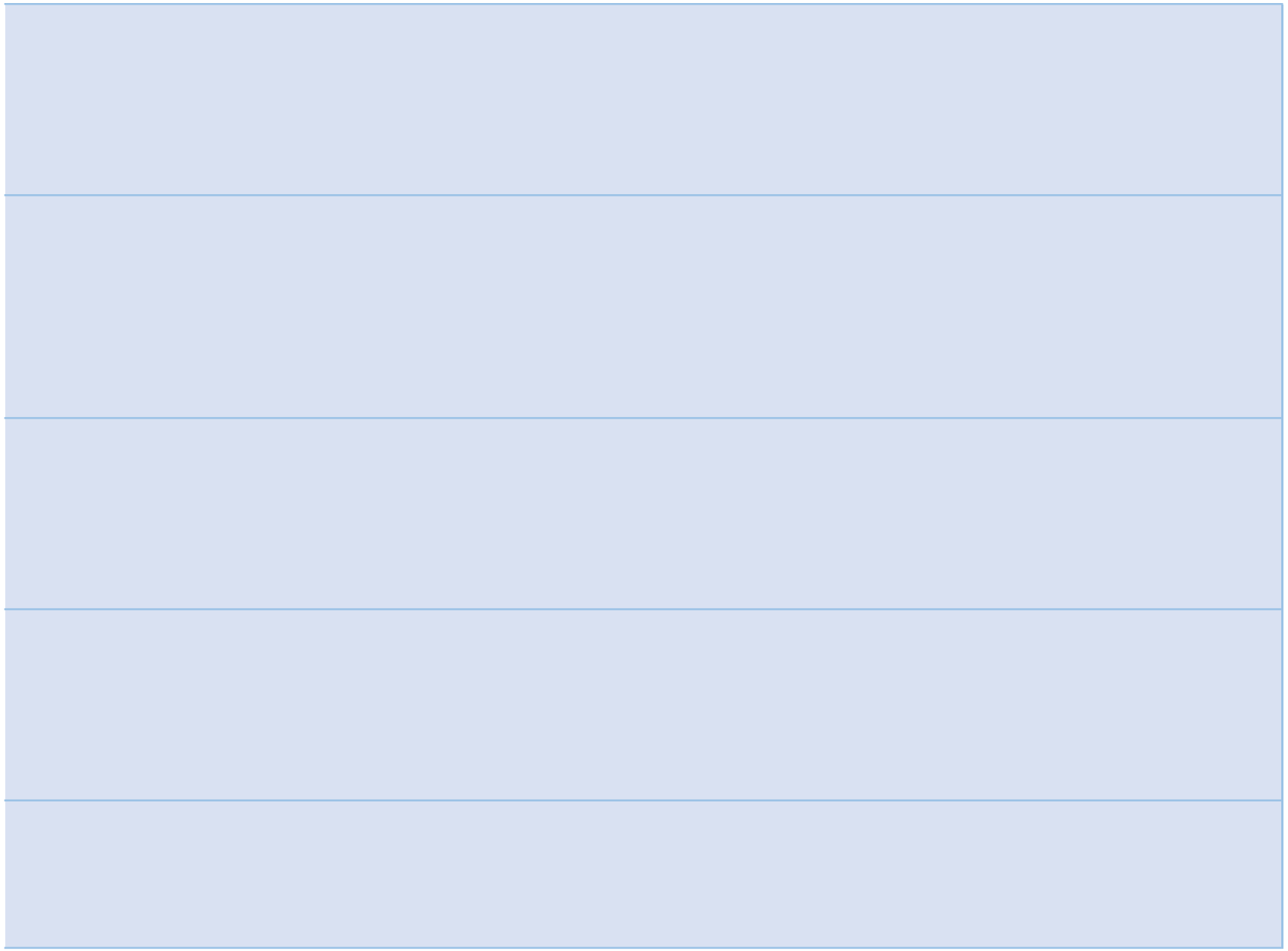


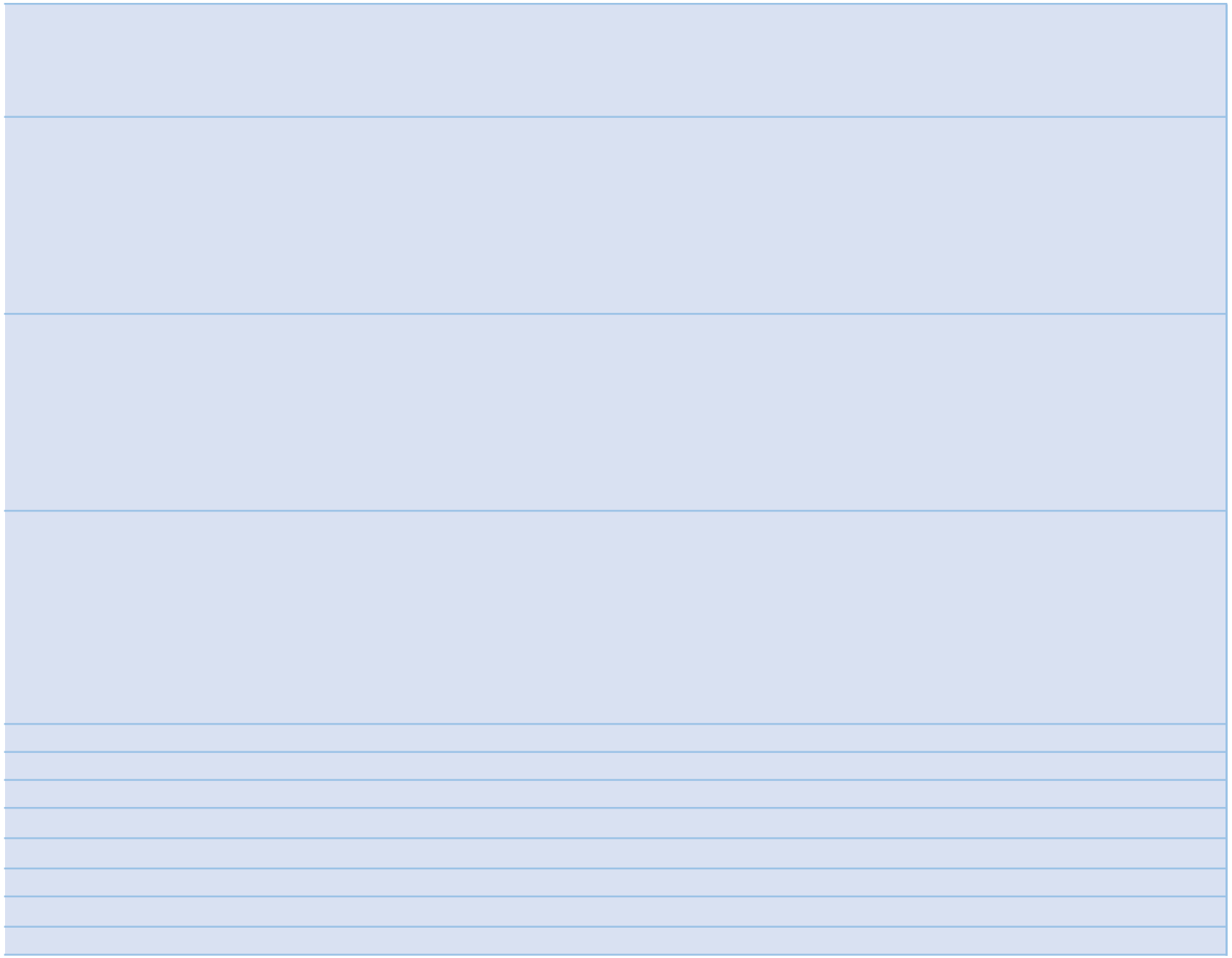


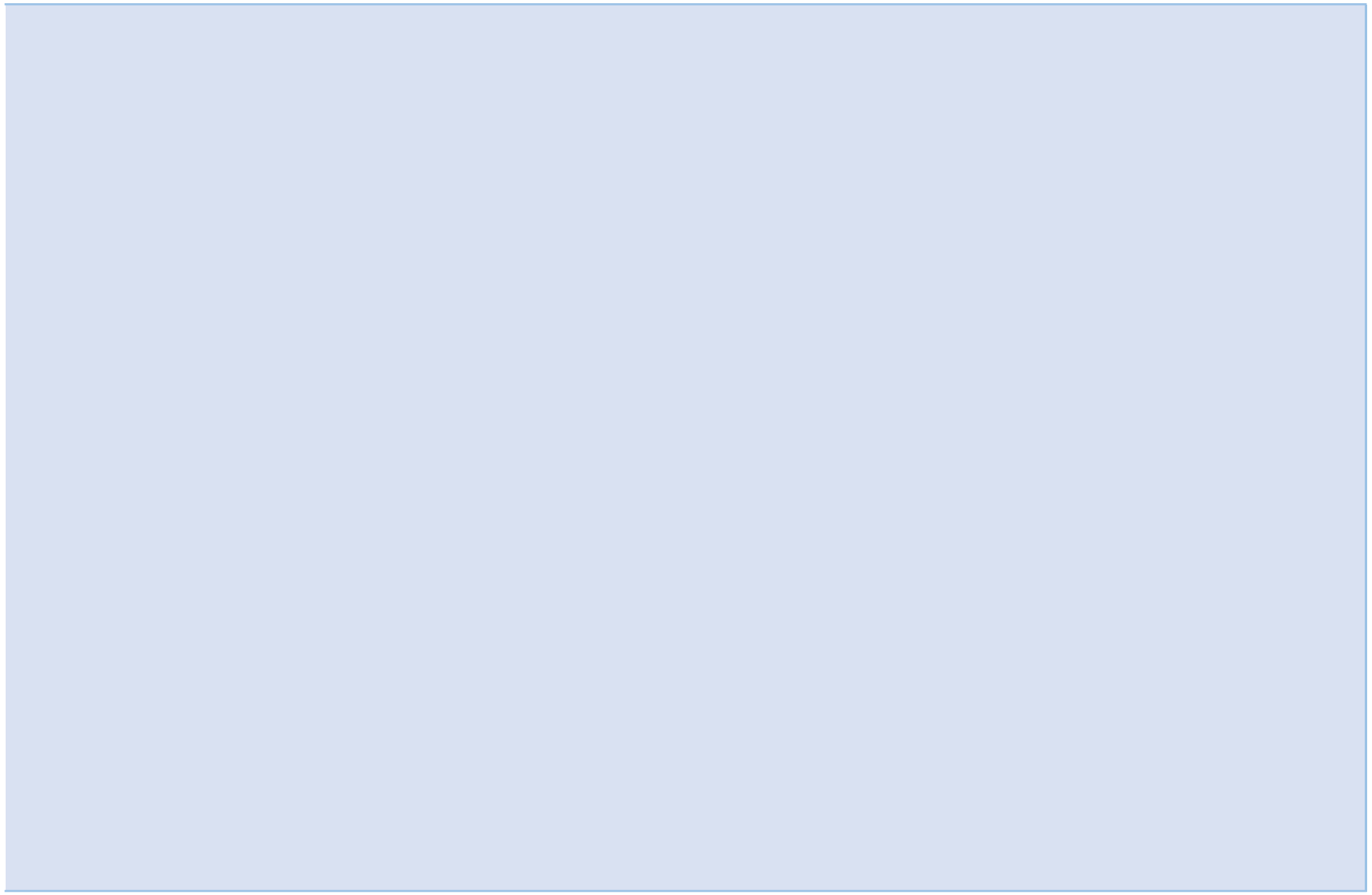


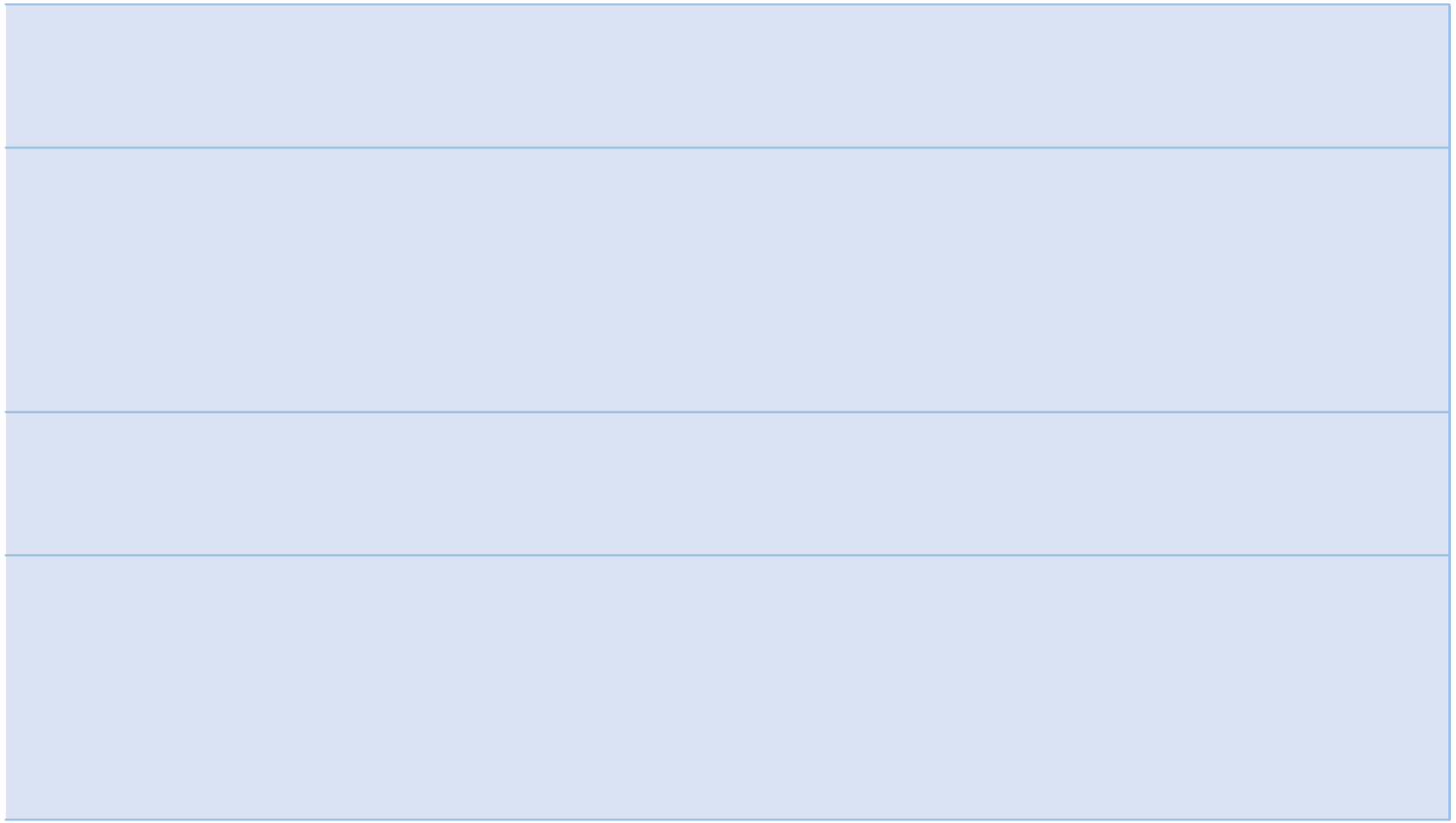


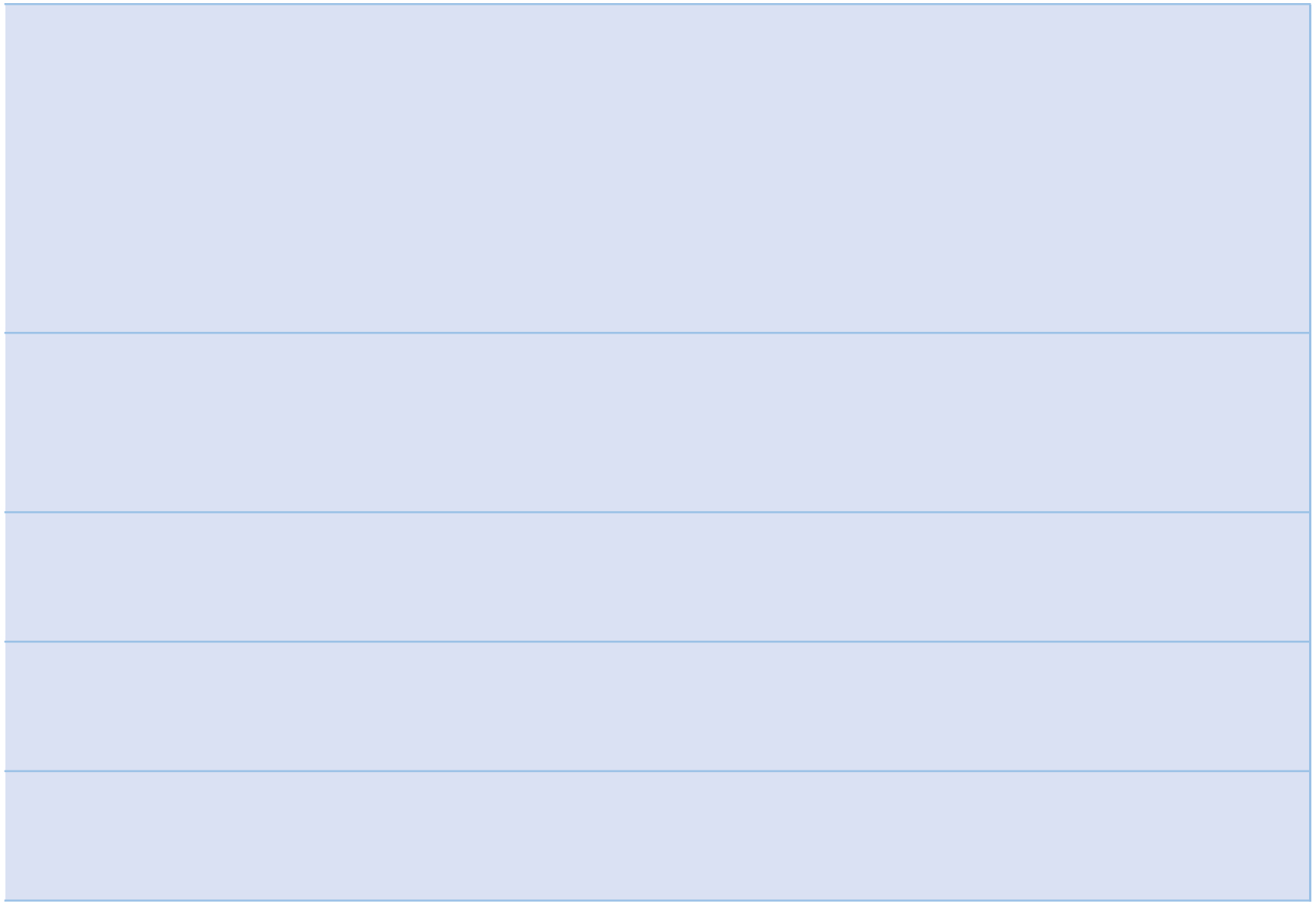


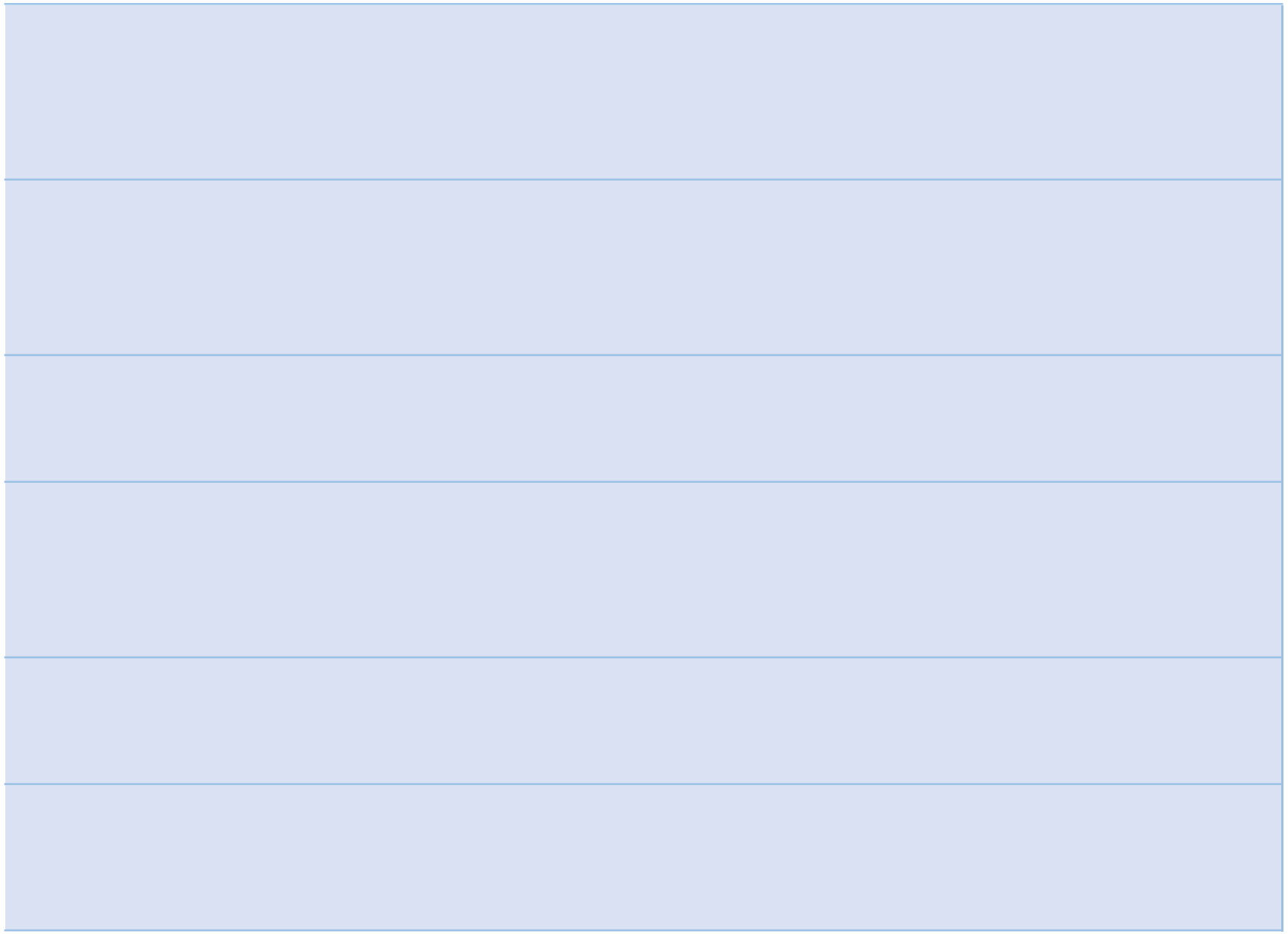


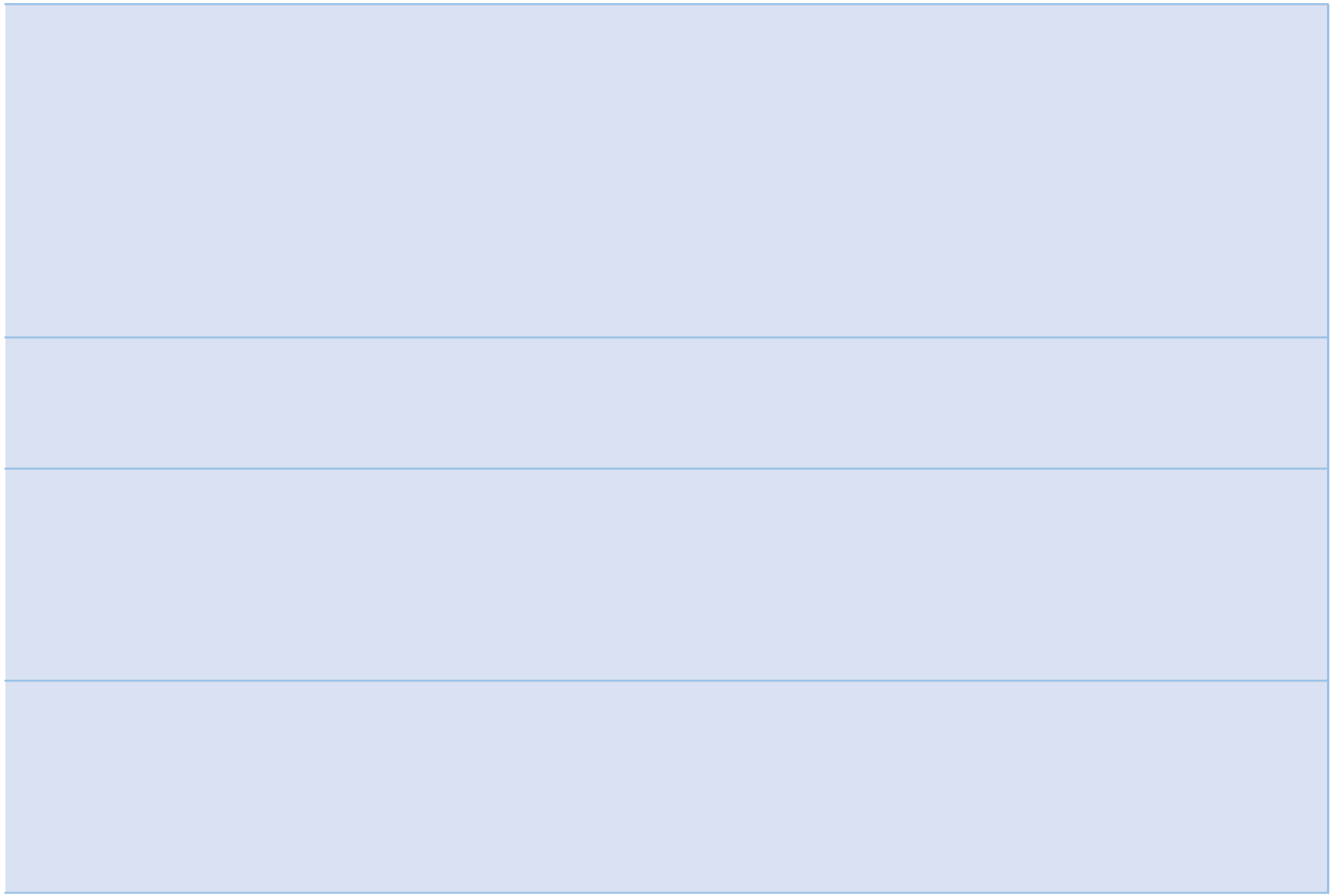


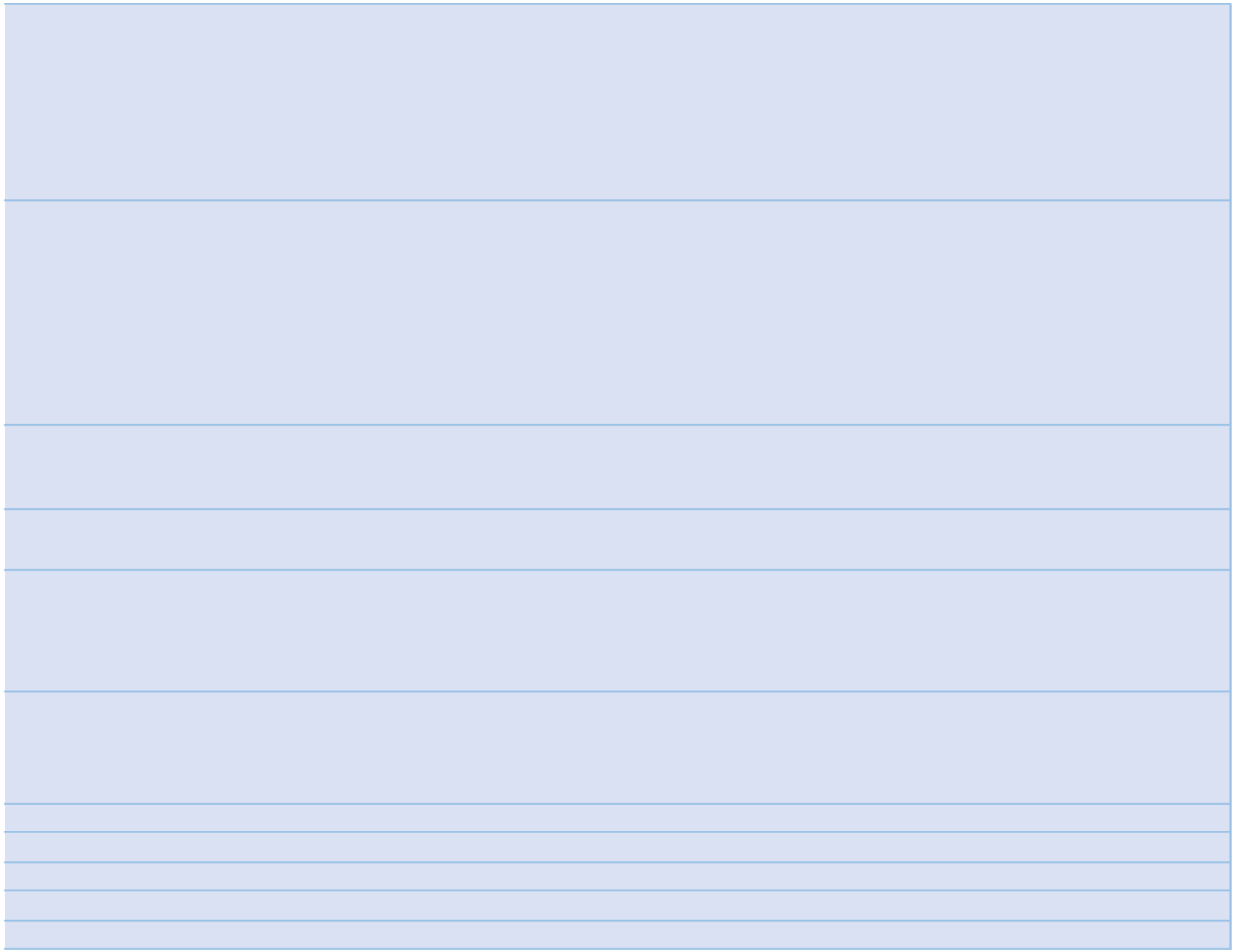








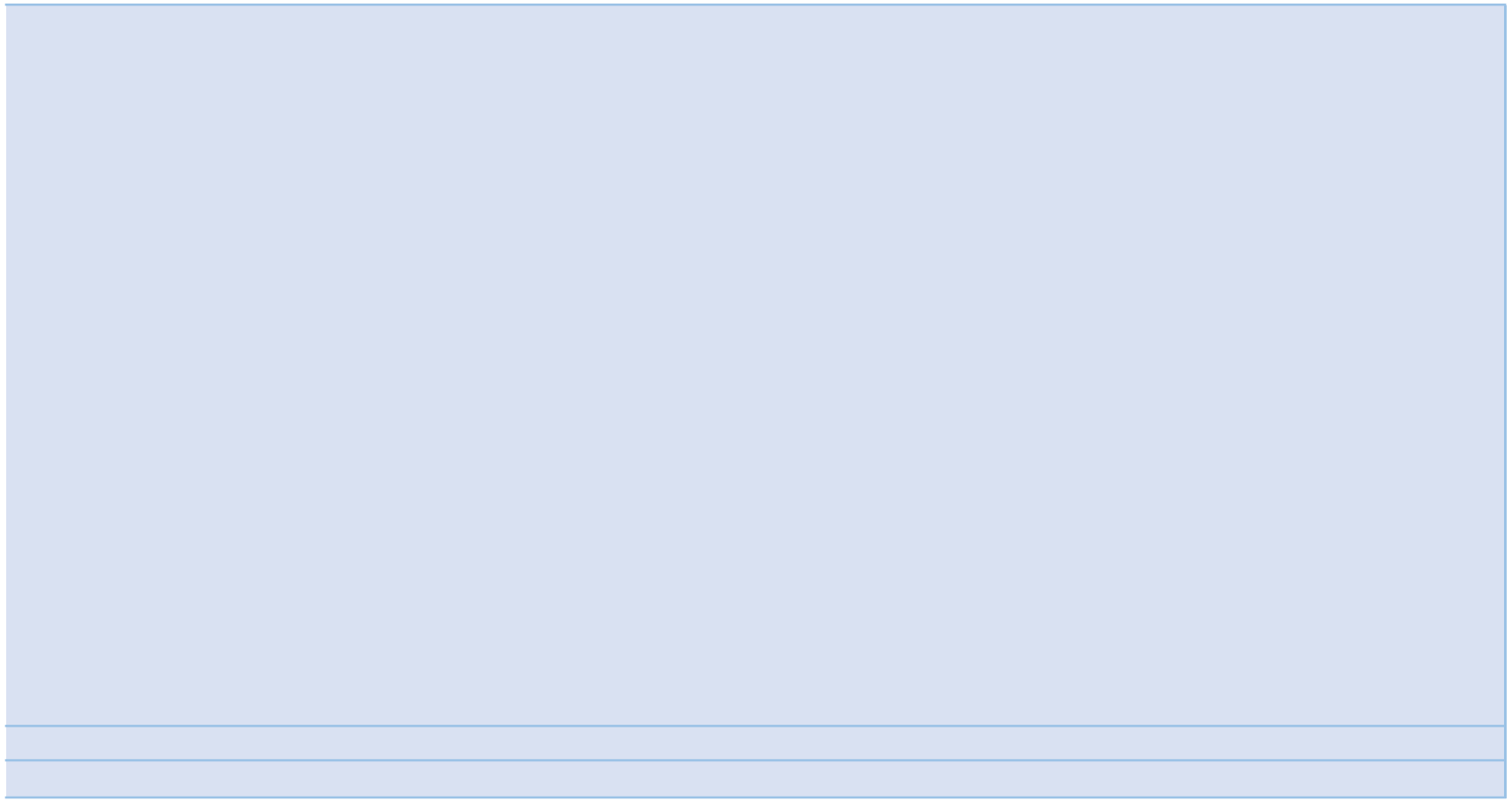


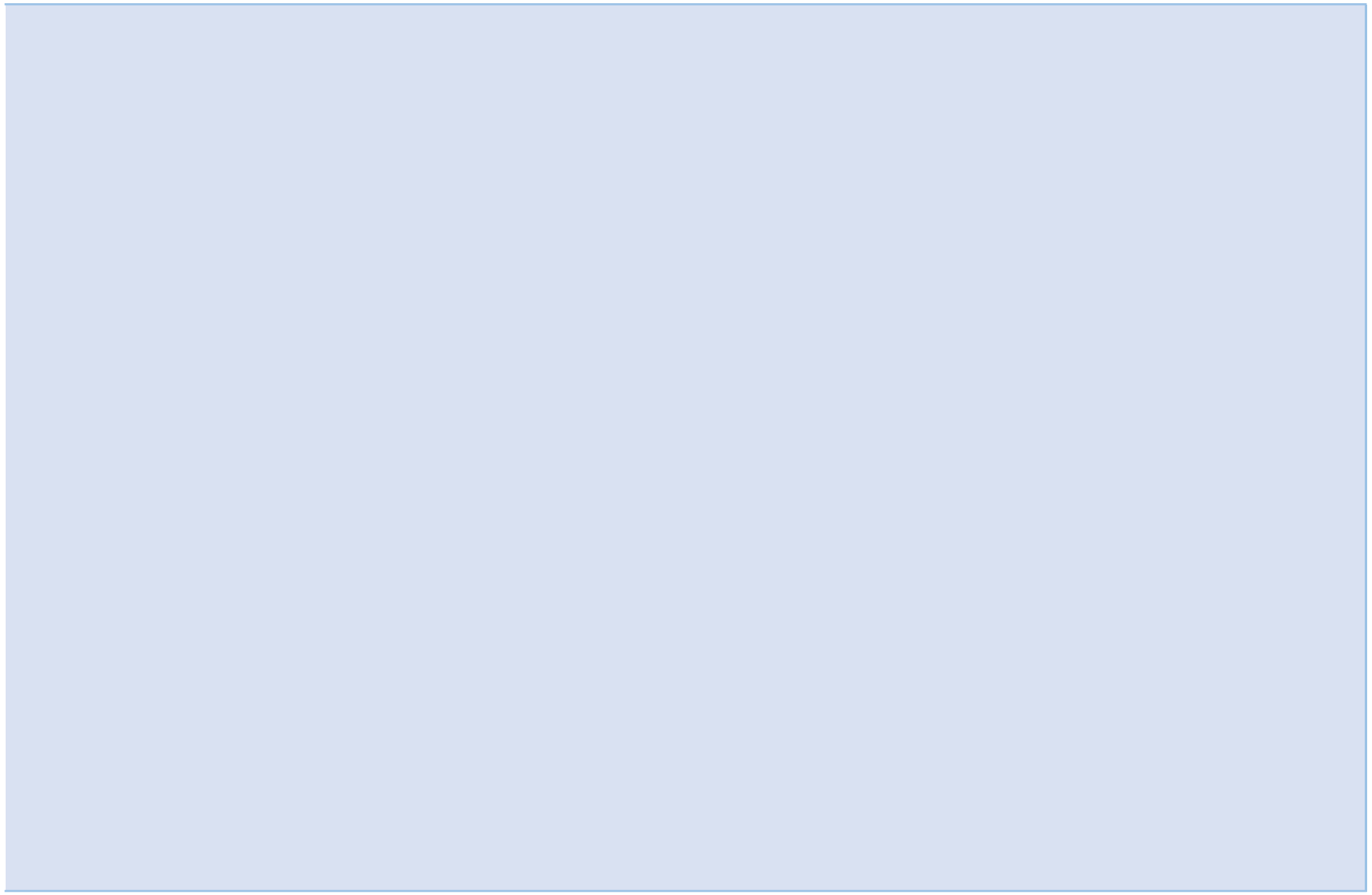


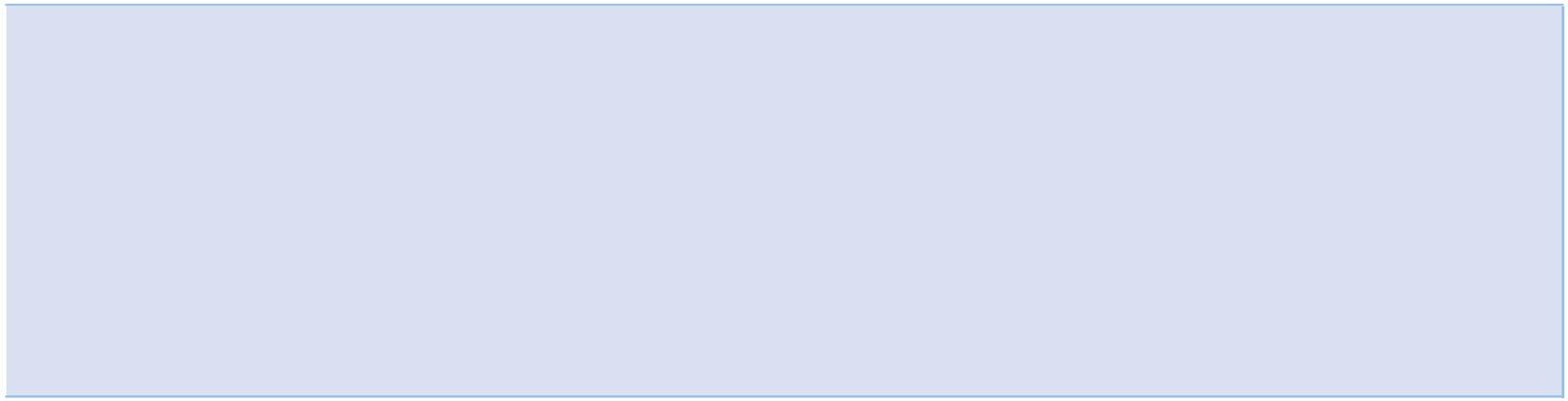
2024-2025

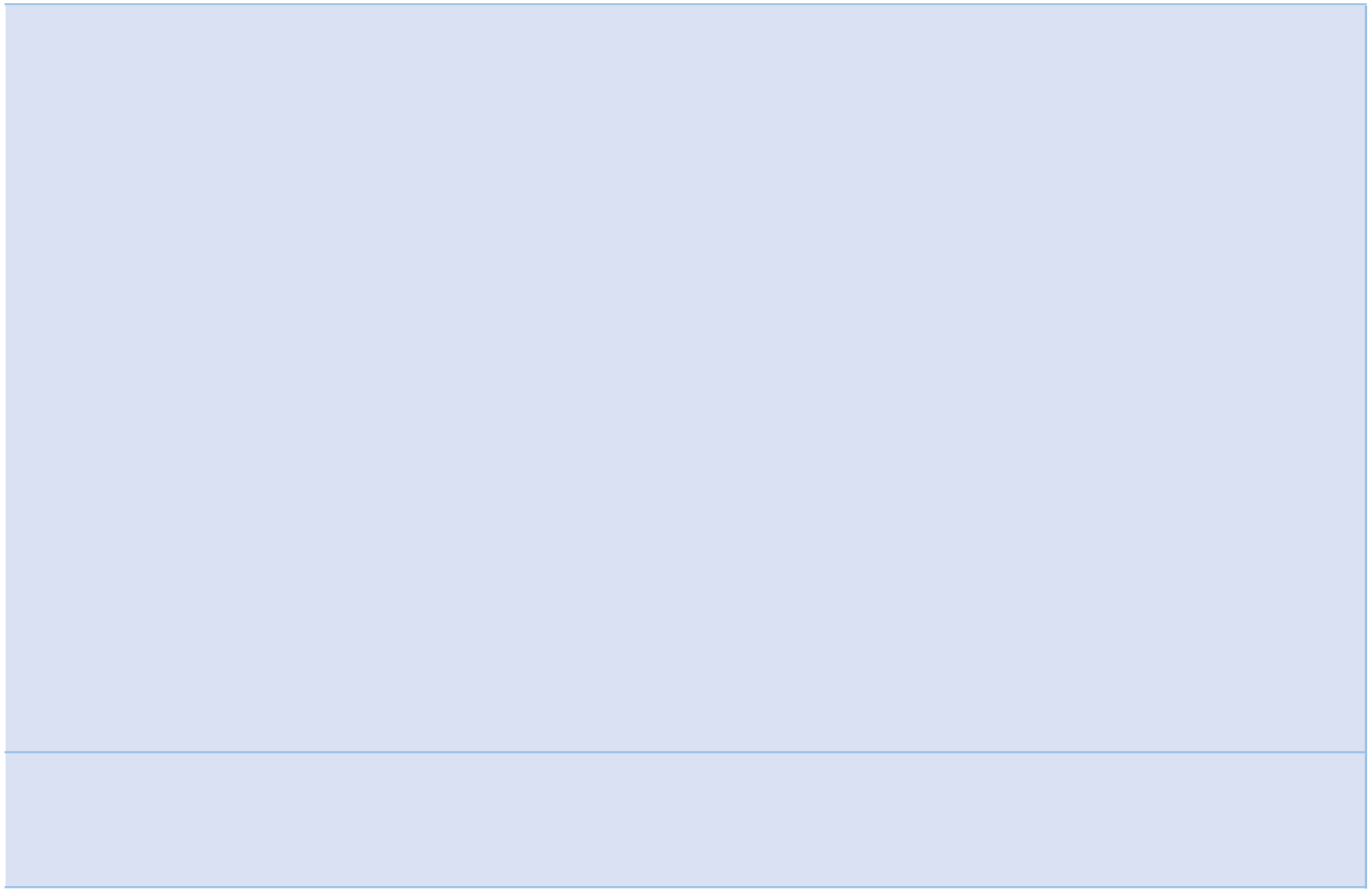
ification 2024-2025

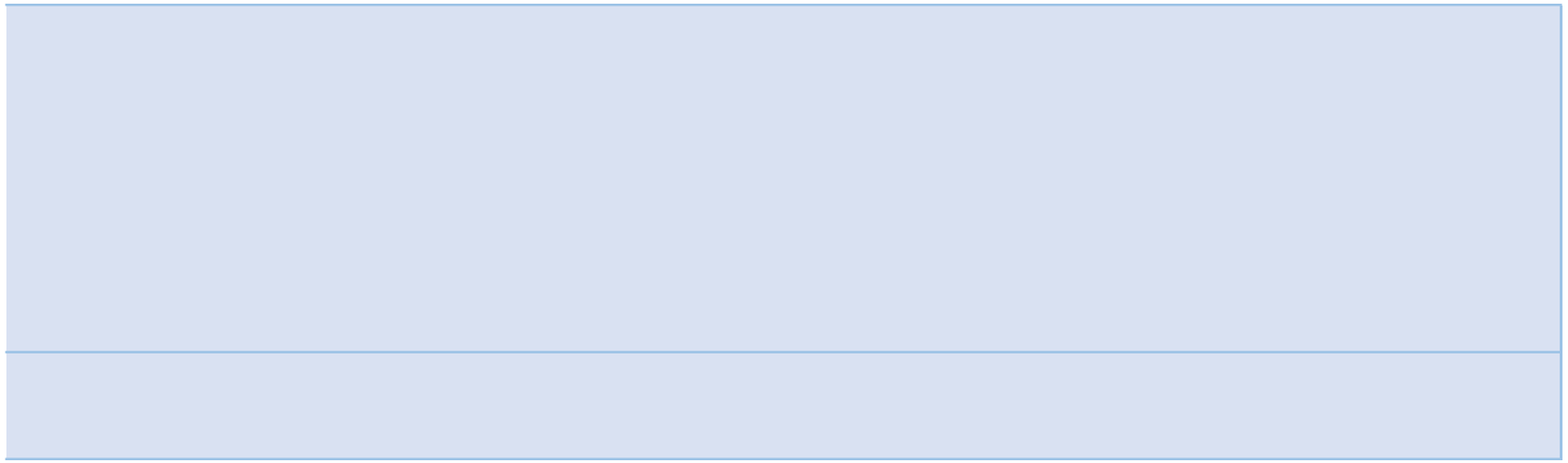
5

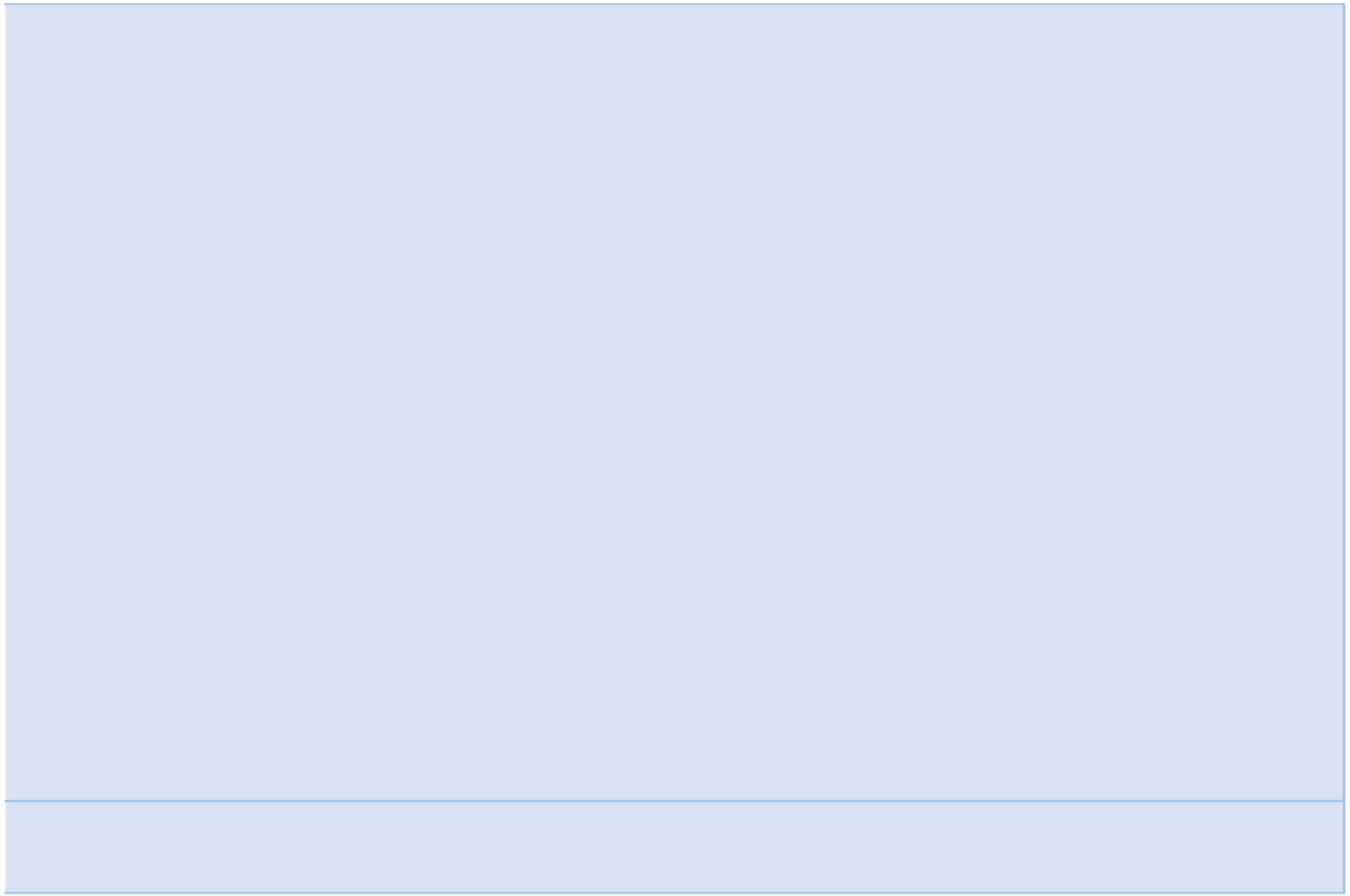


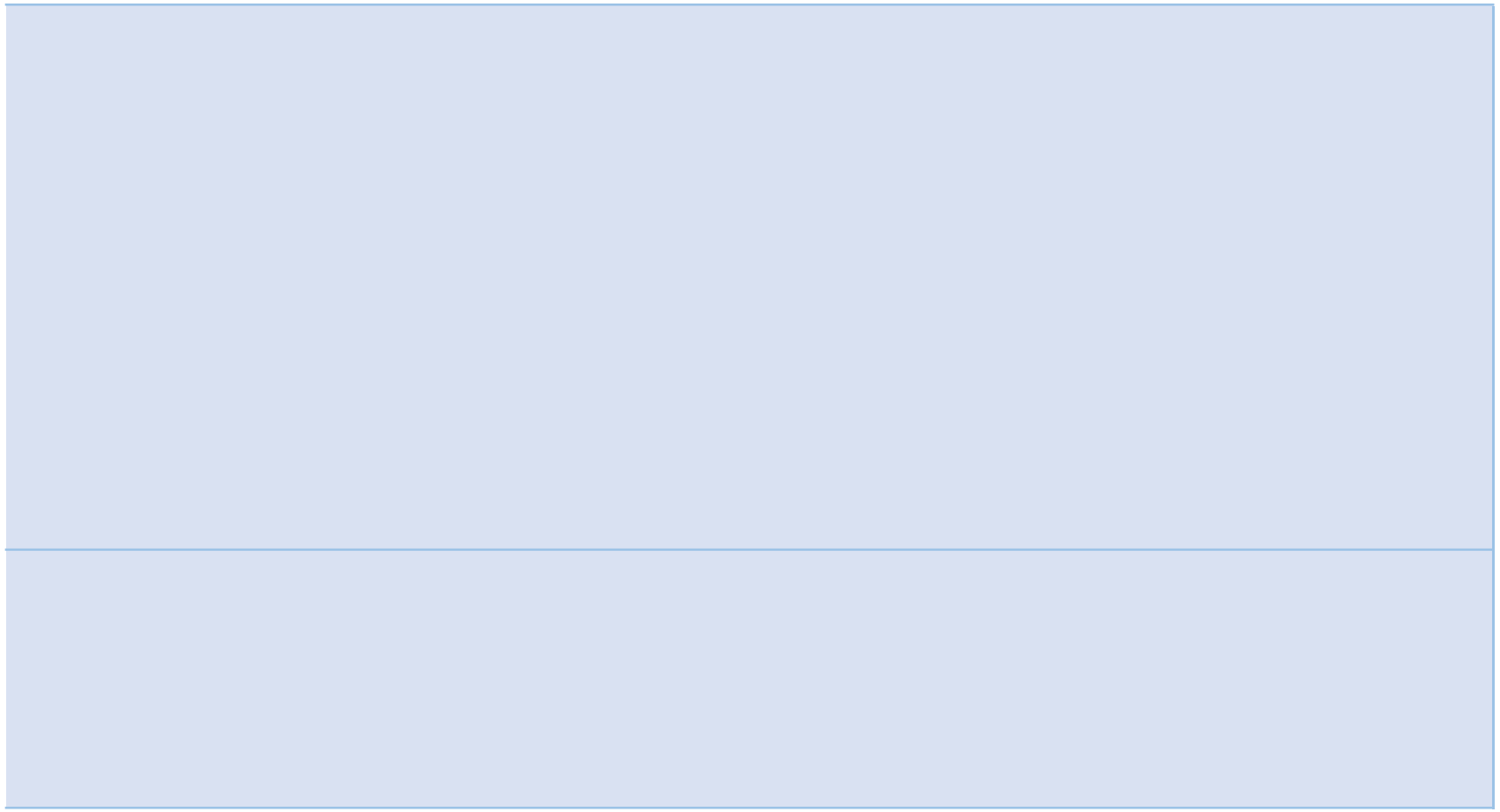


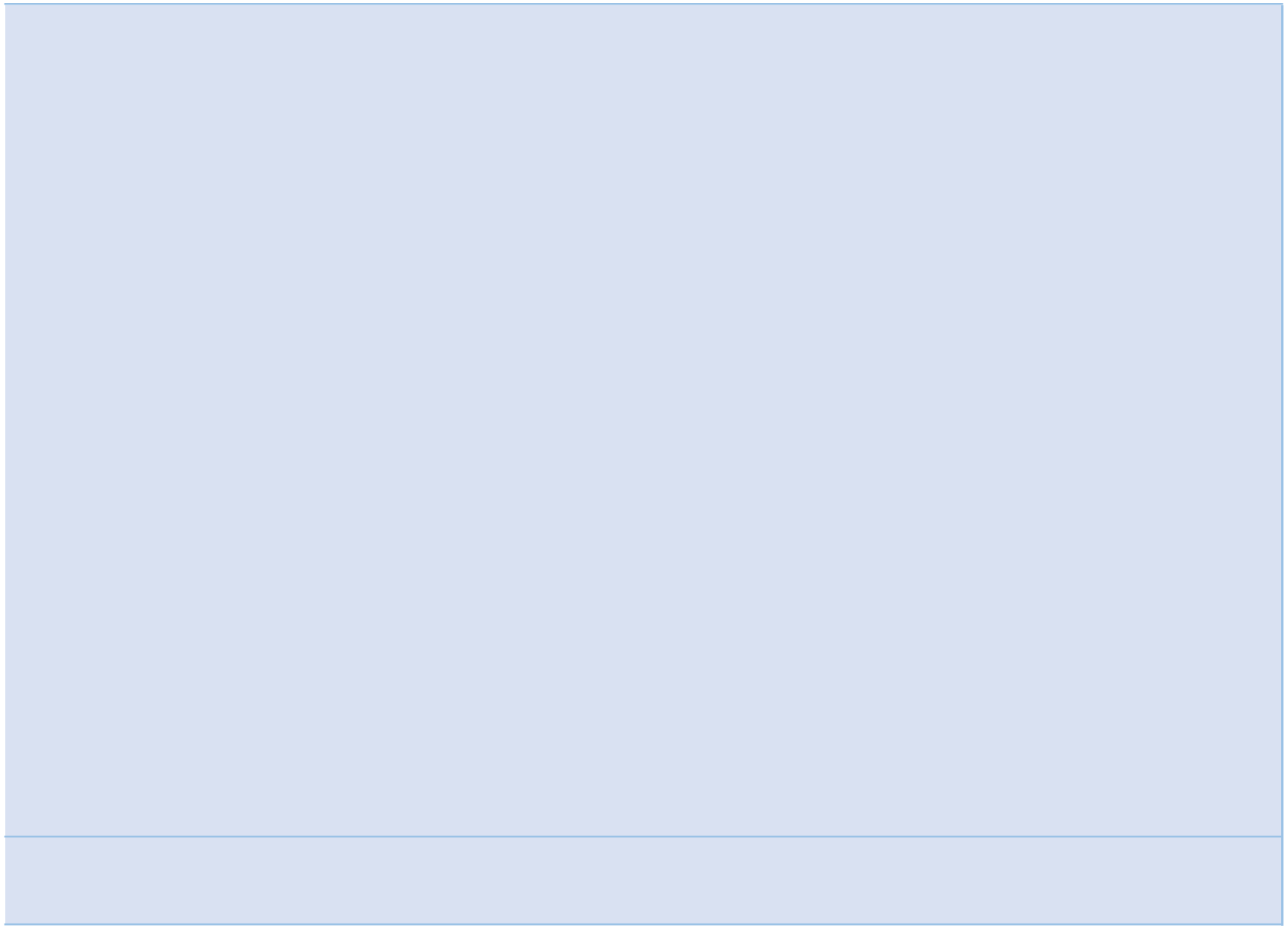


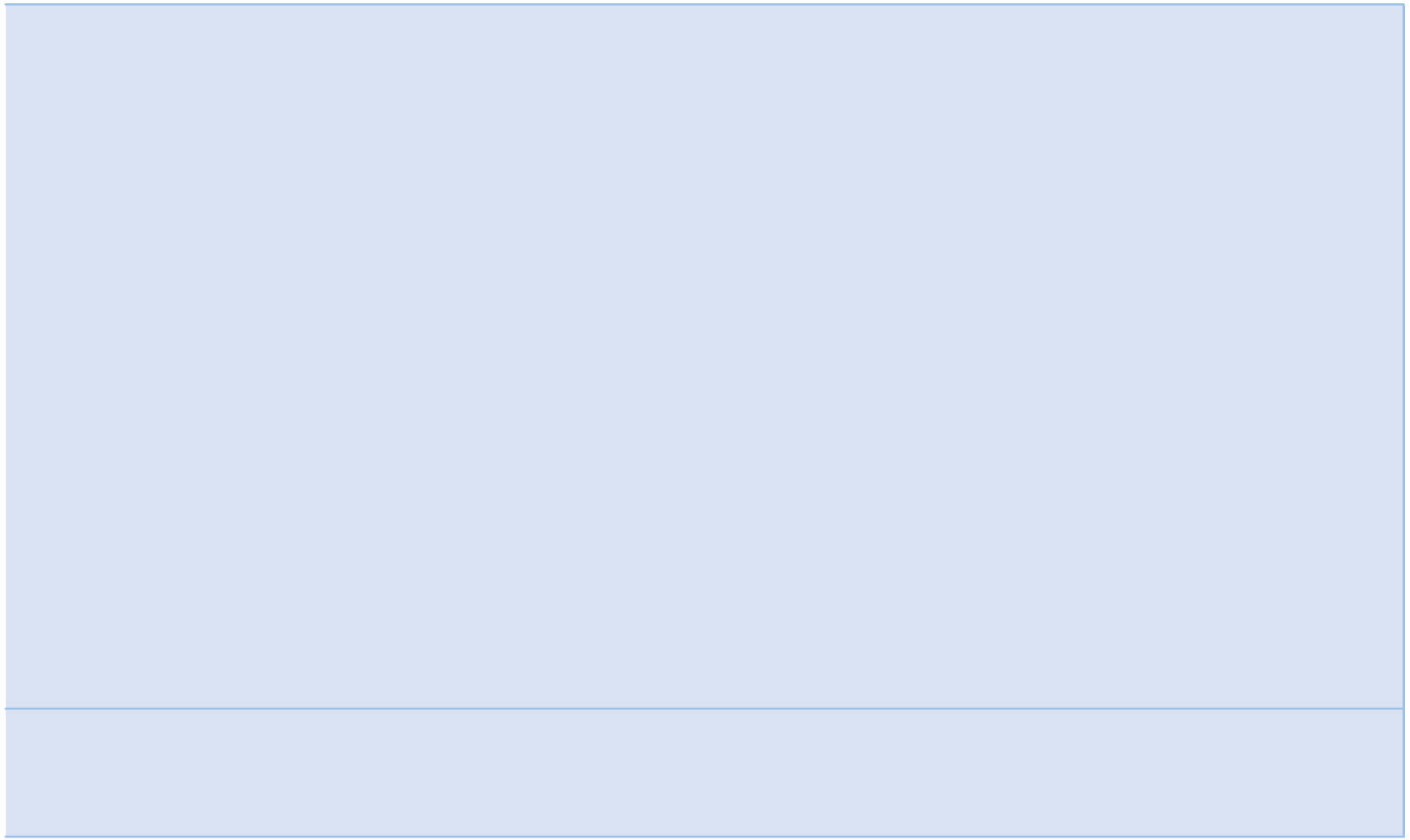


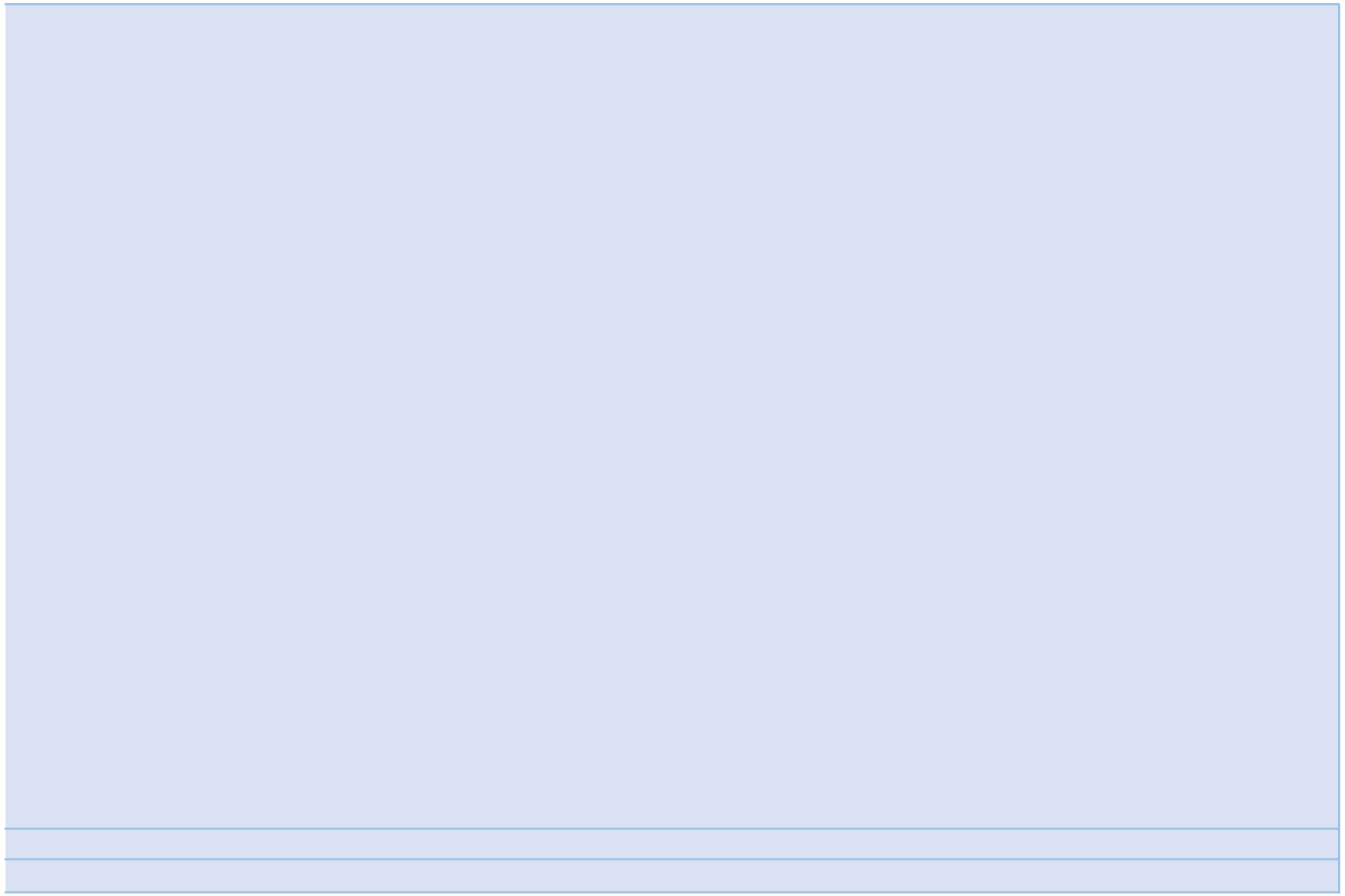


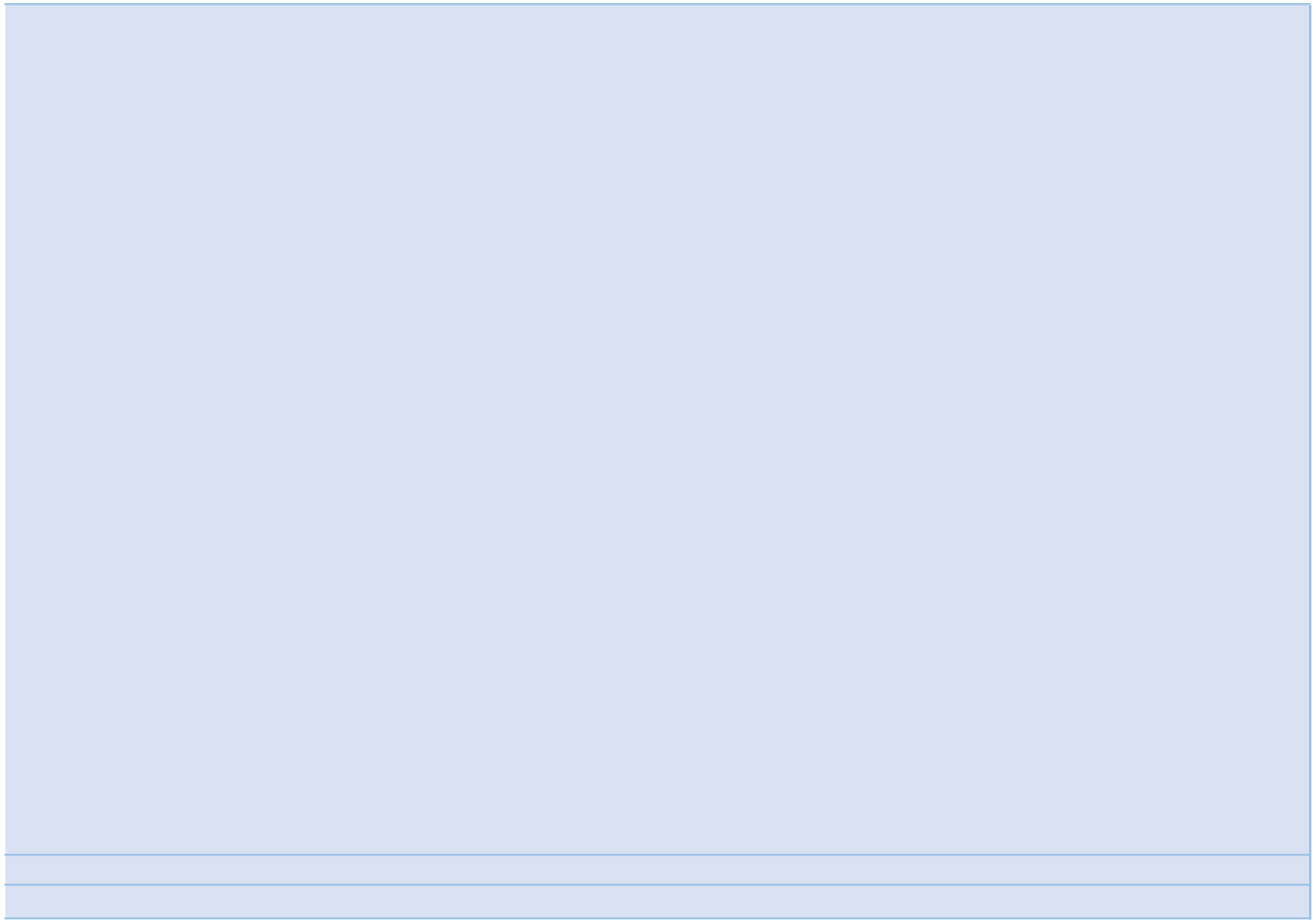


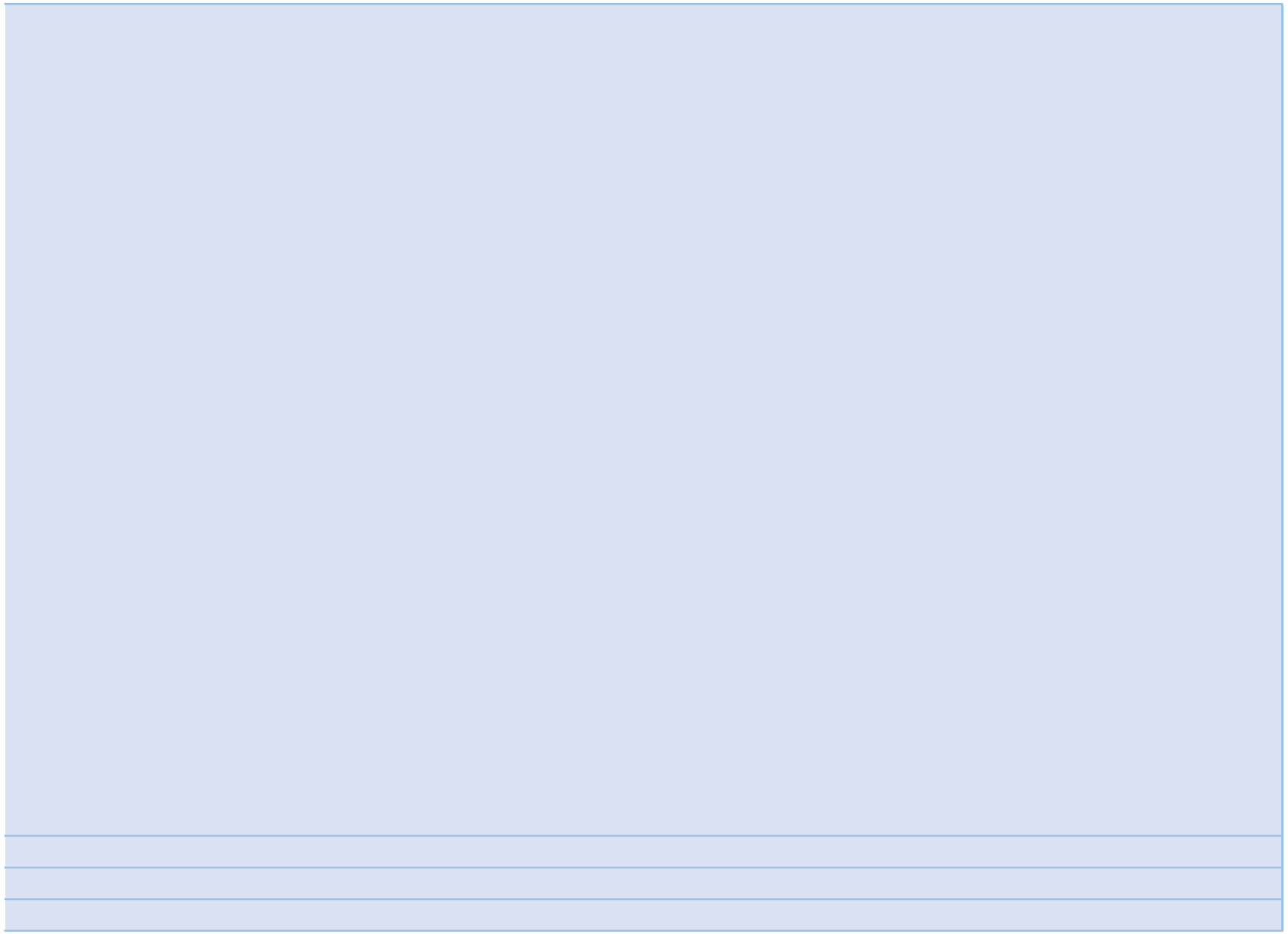


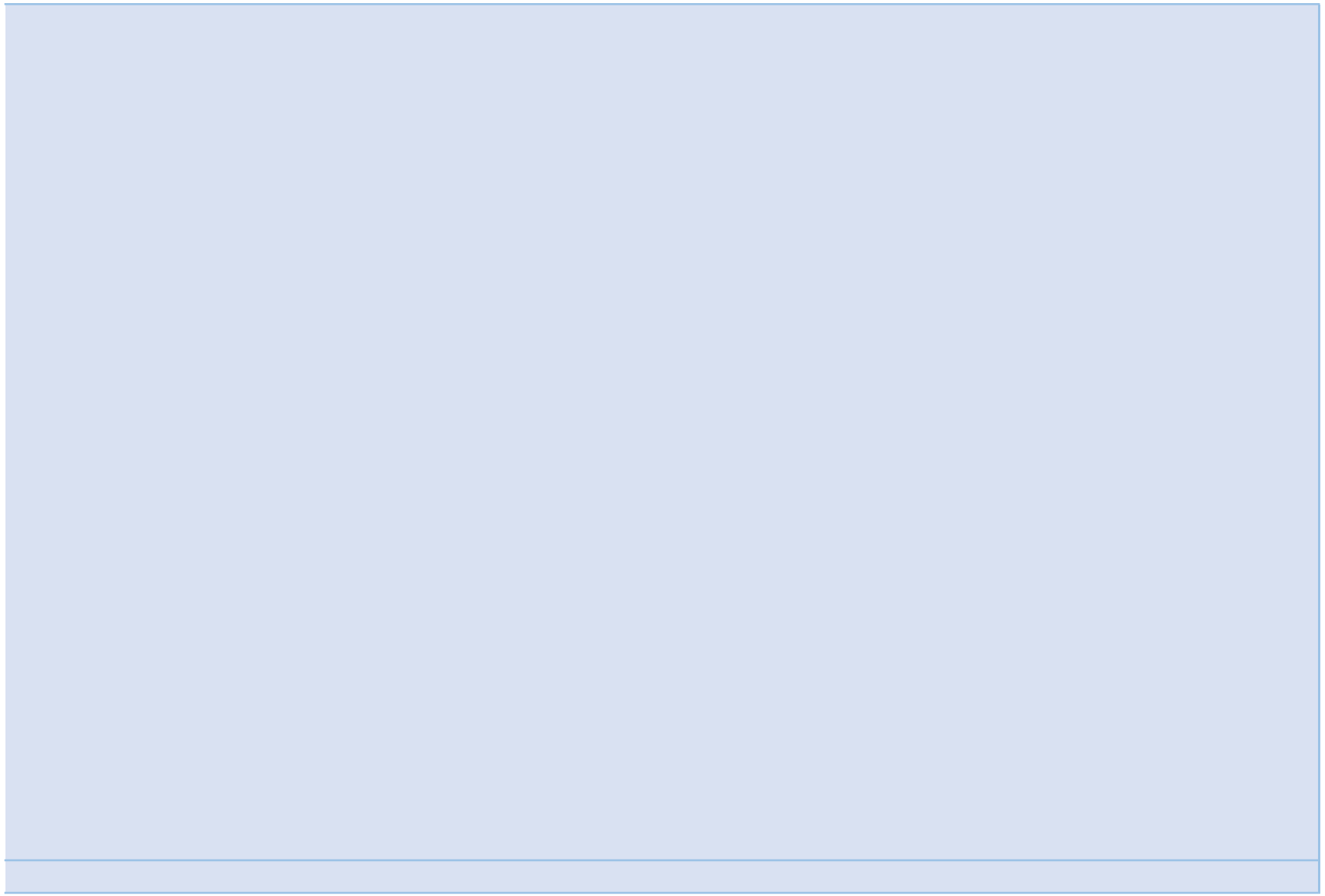


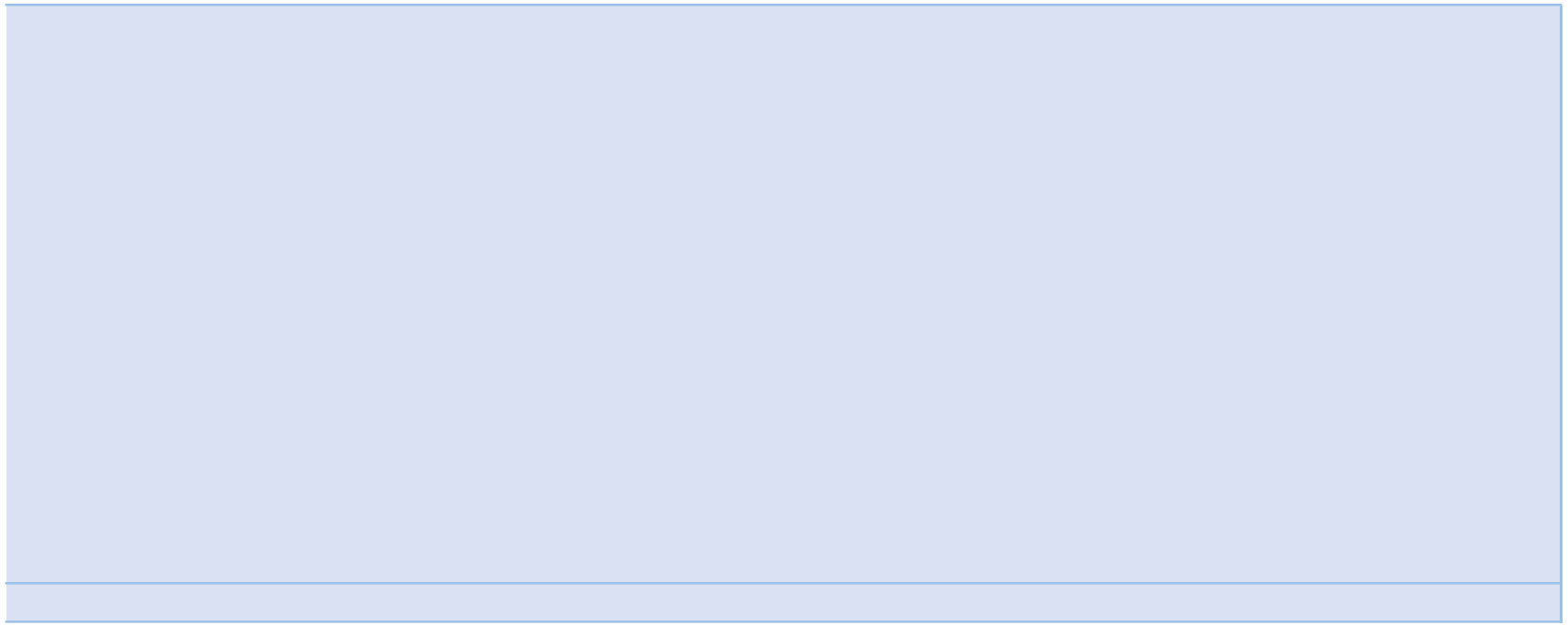


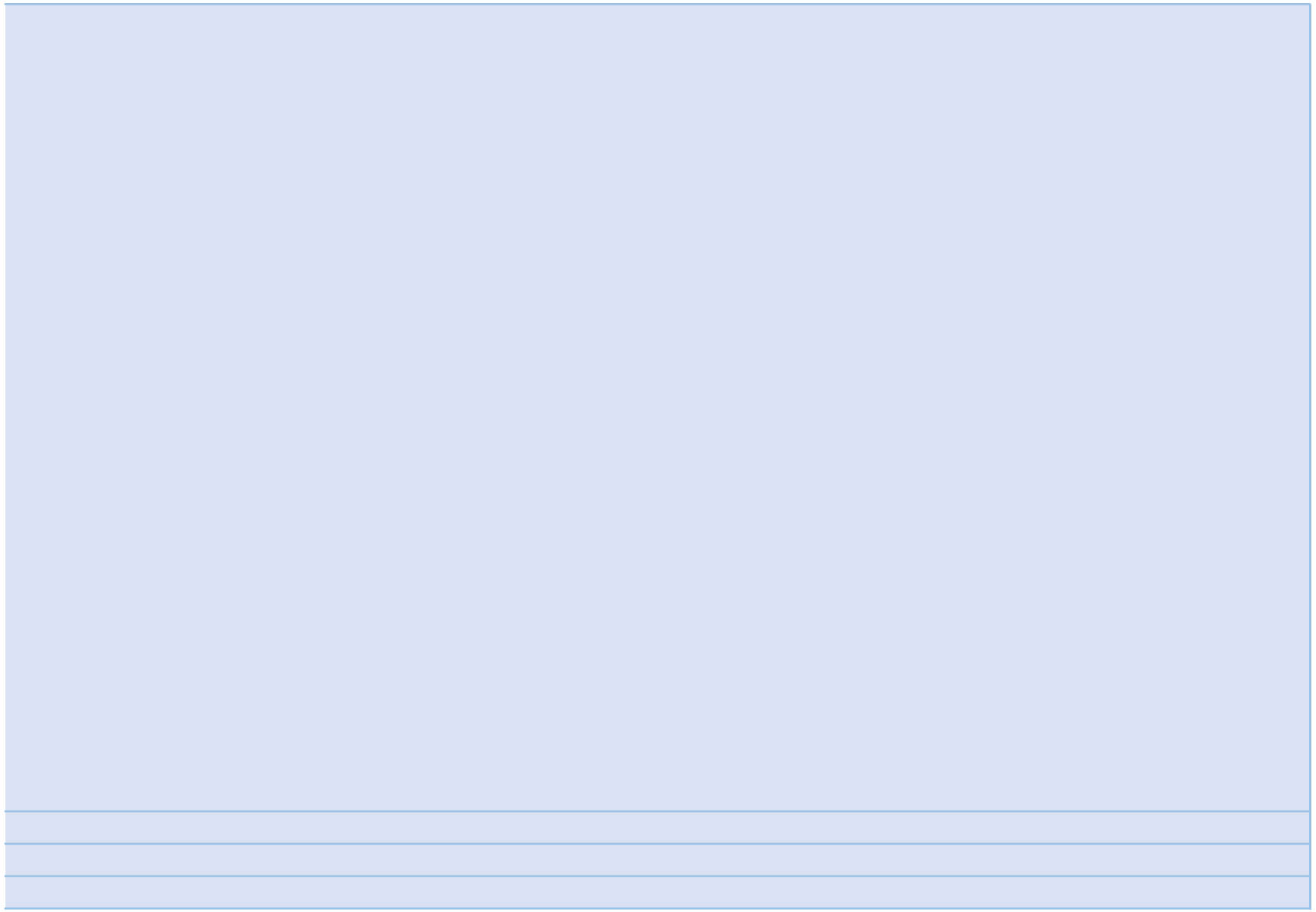


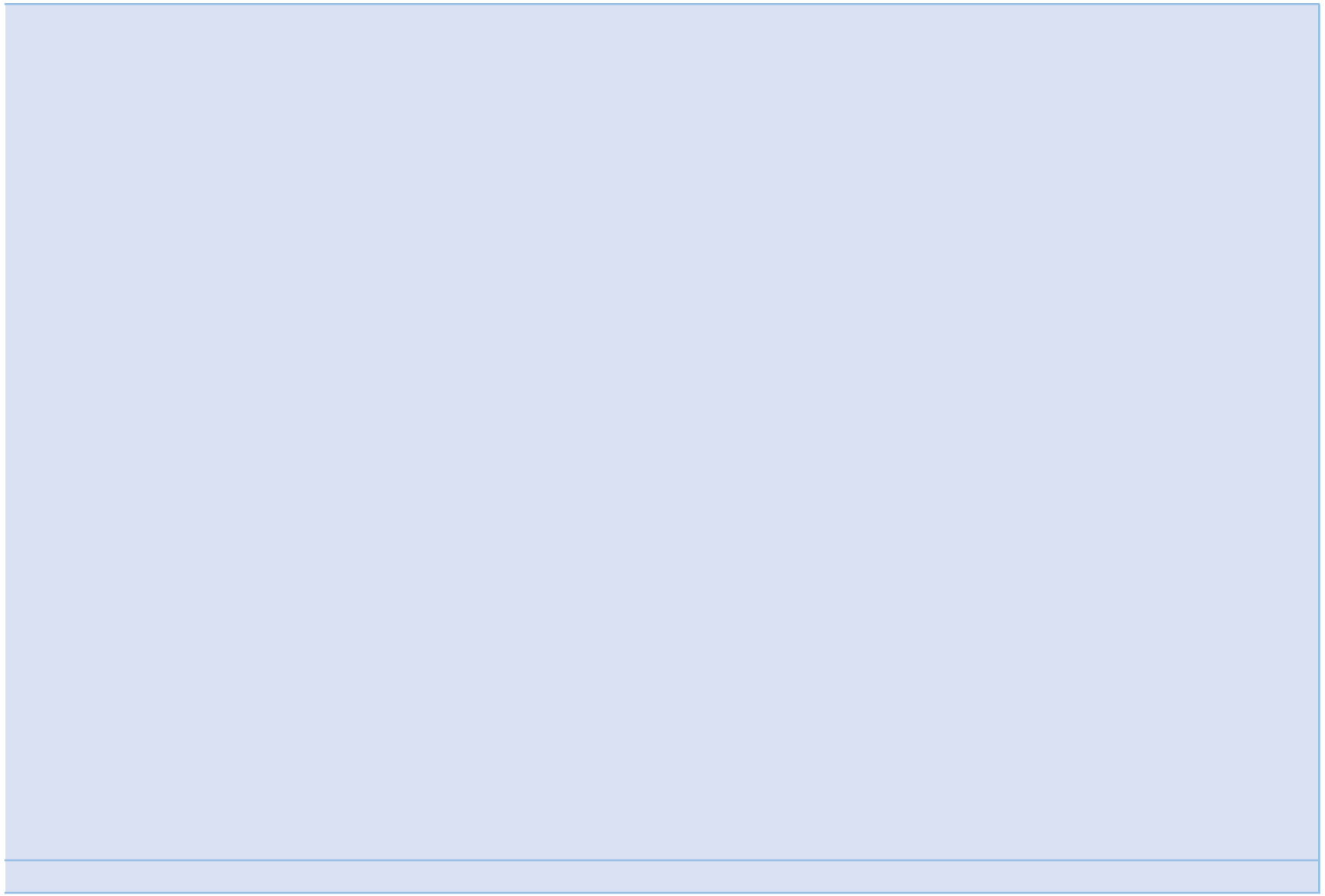


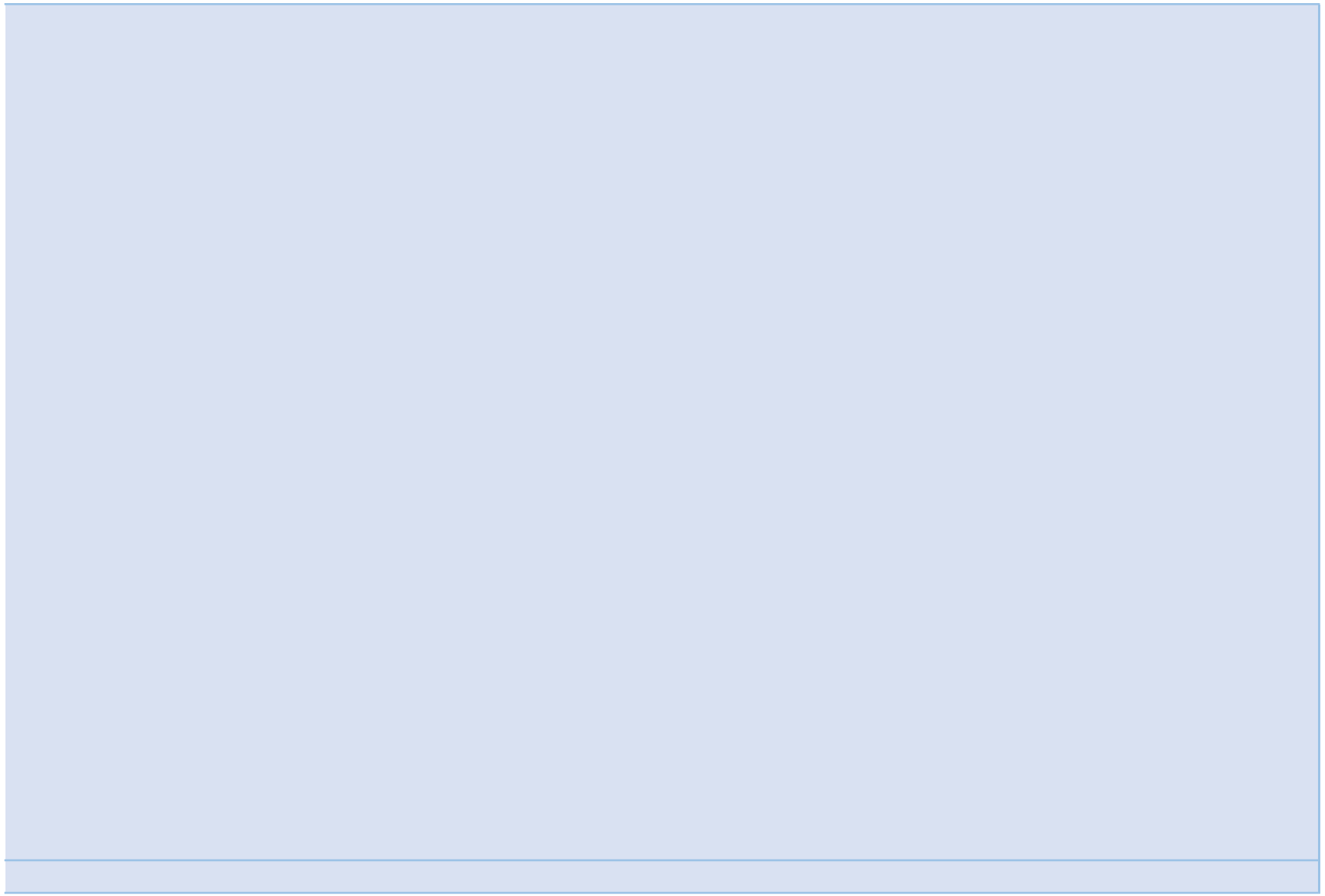


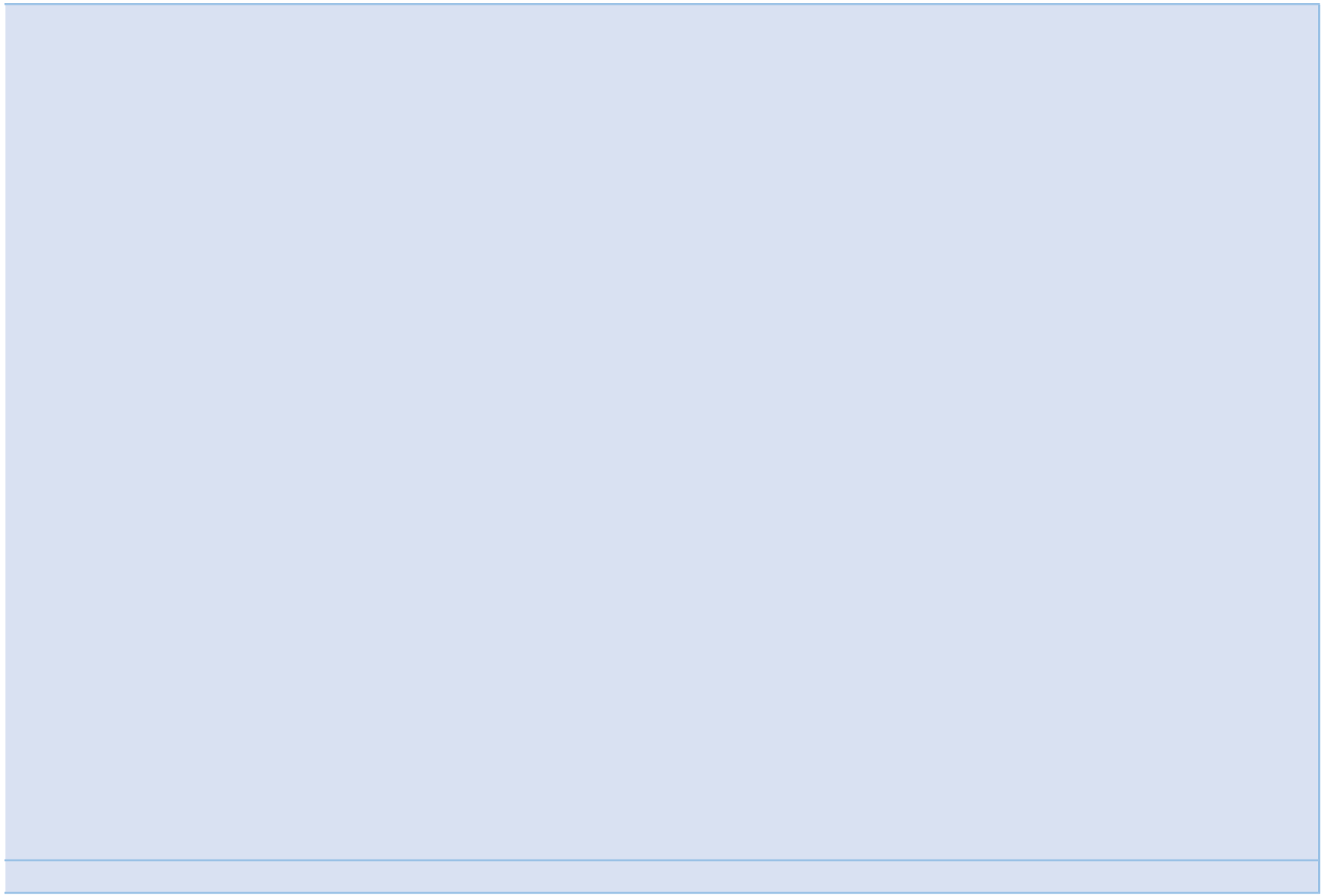


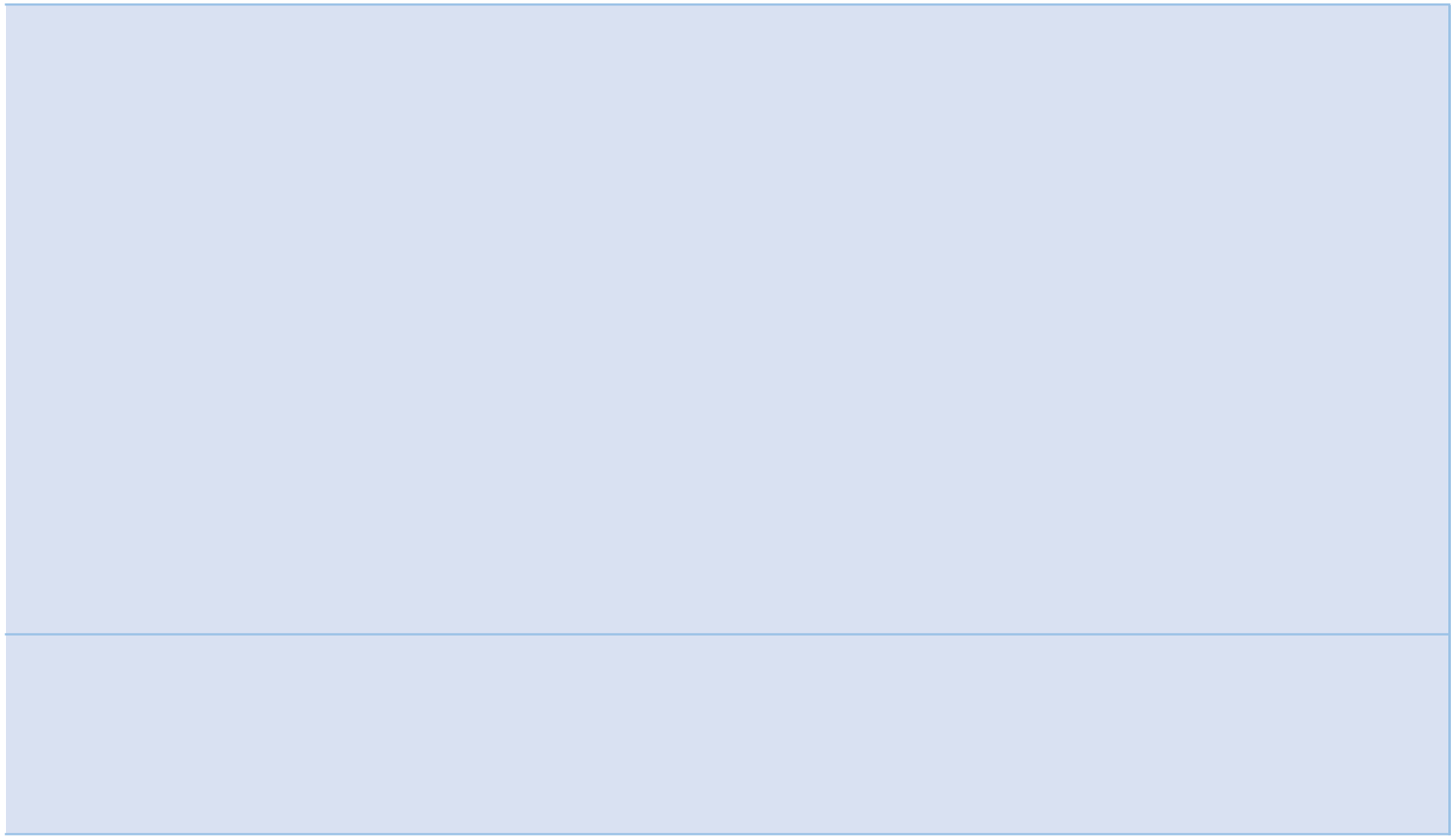


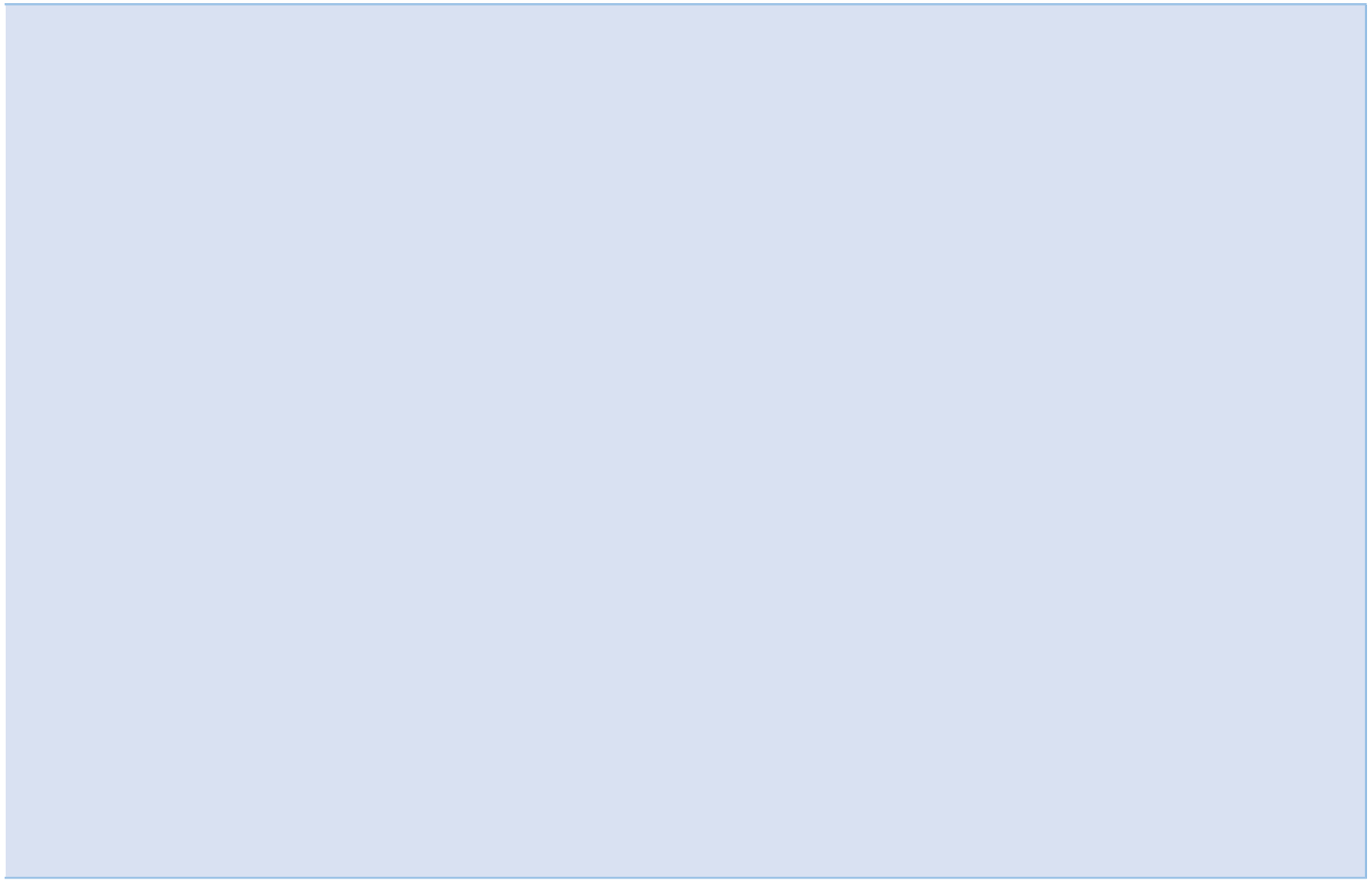


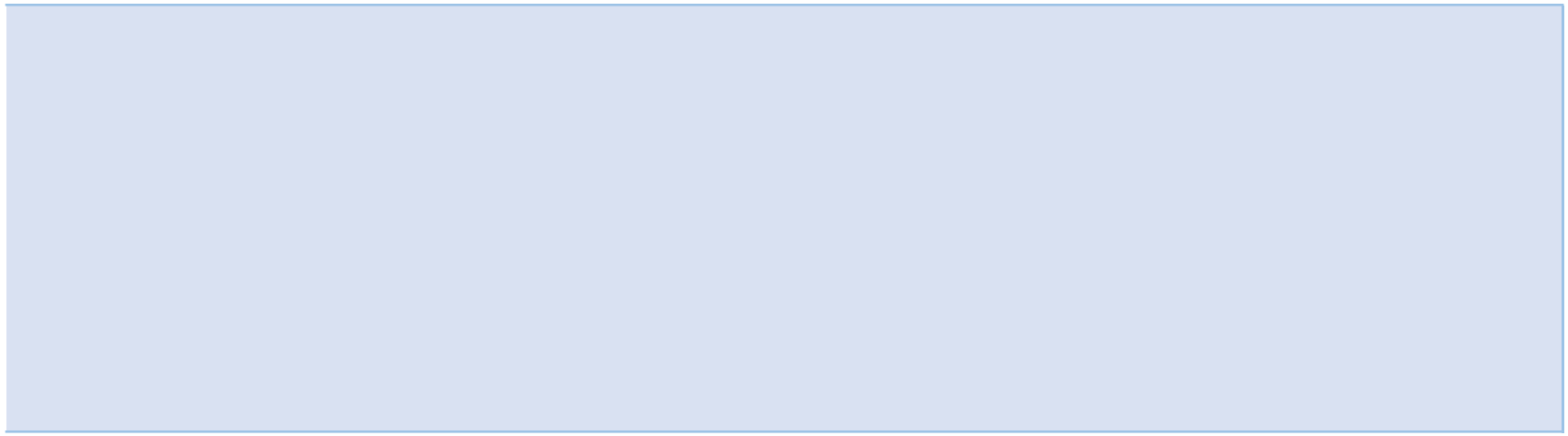


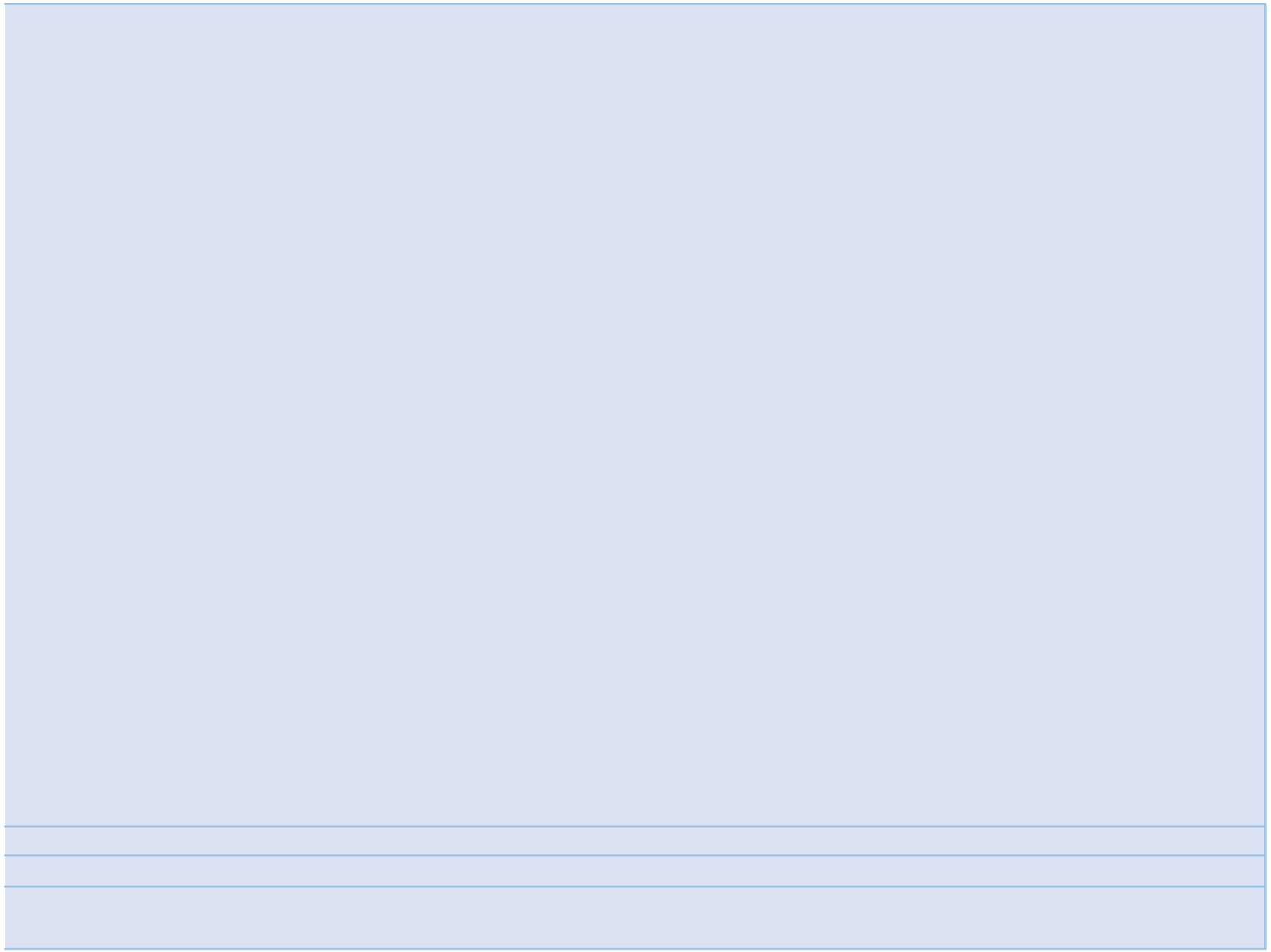


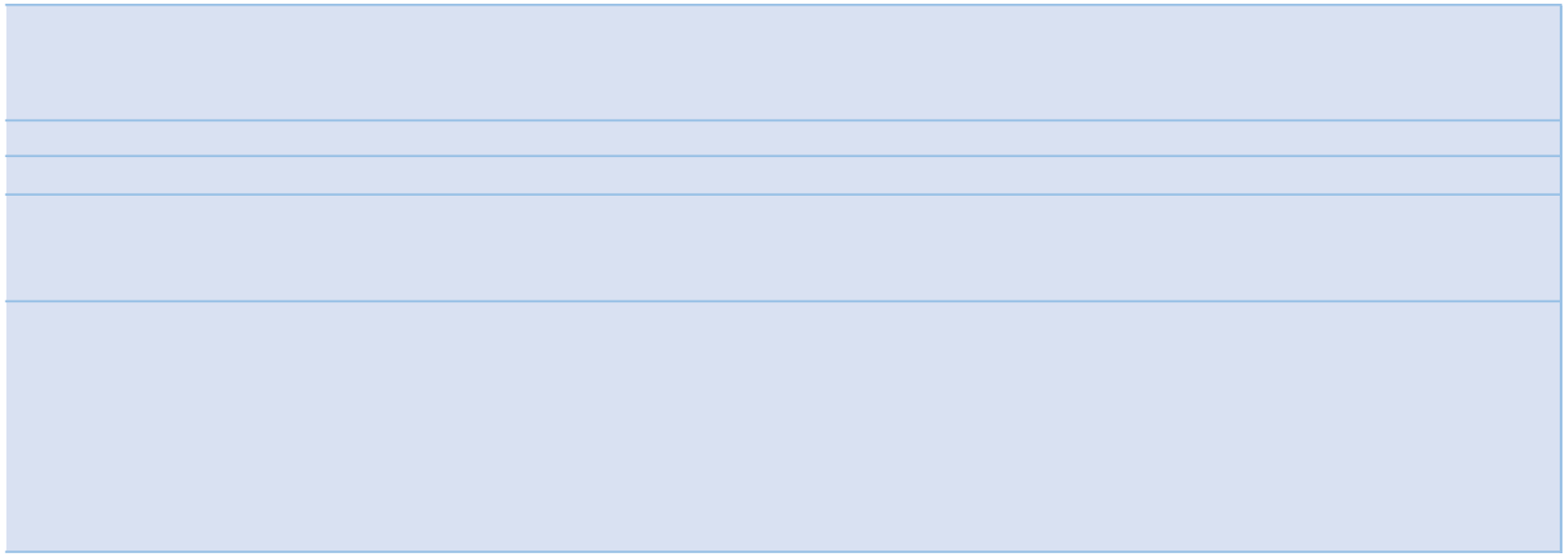


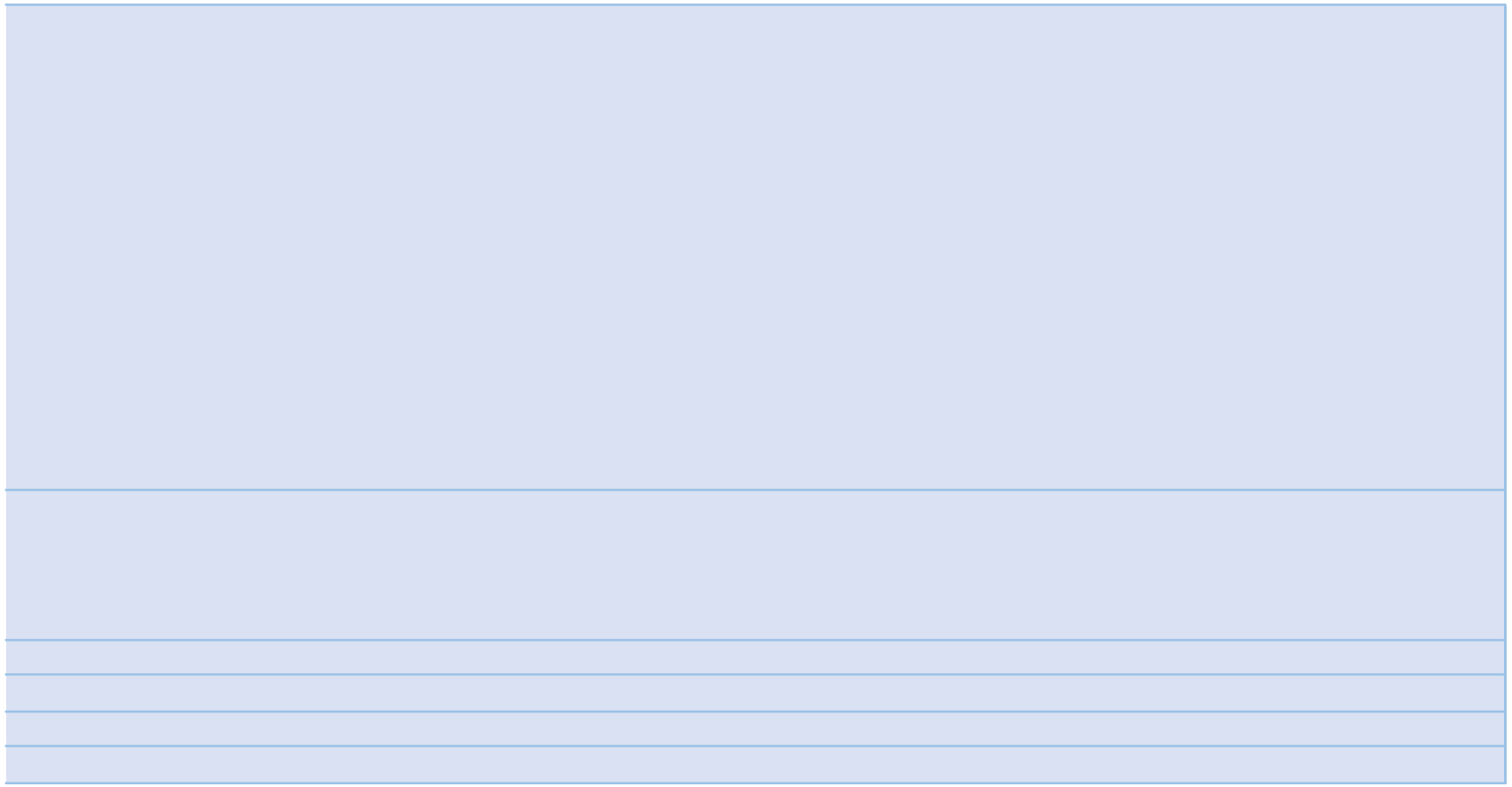


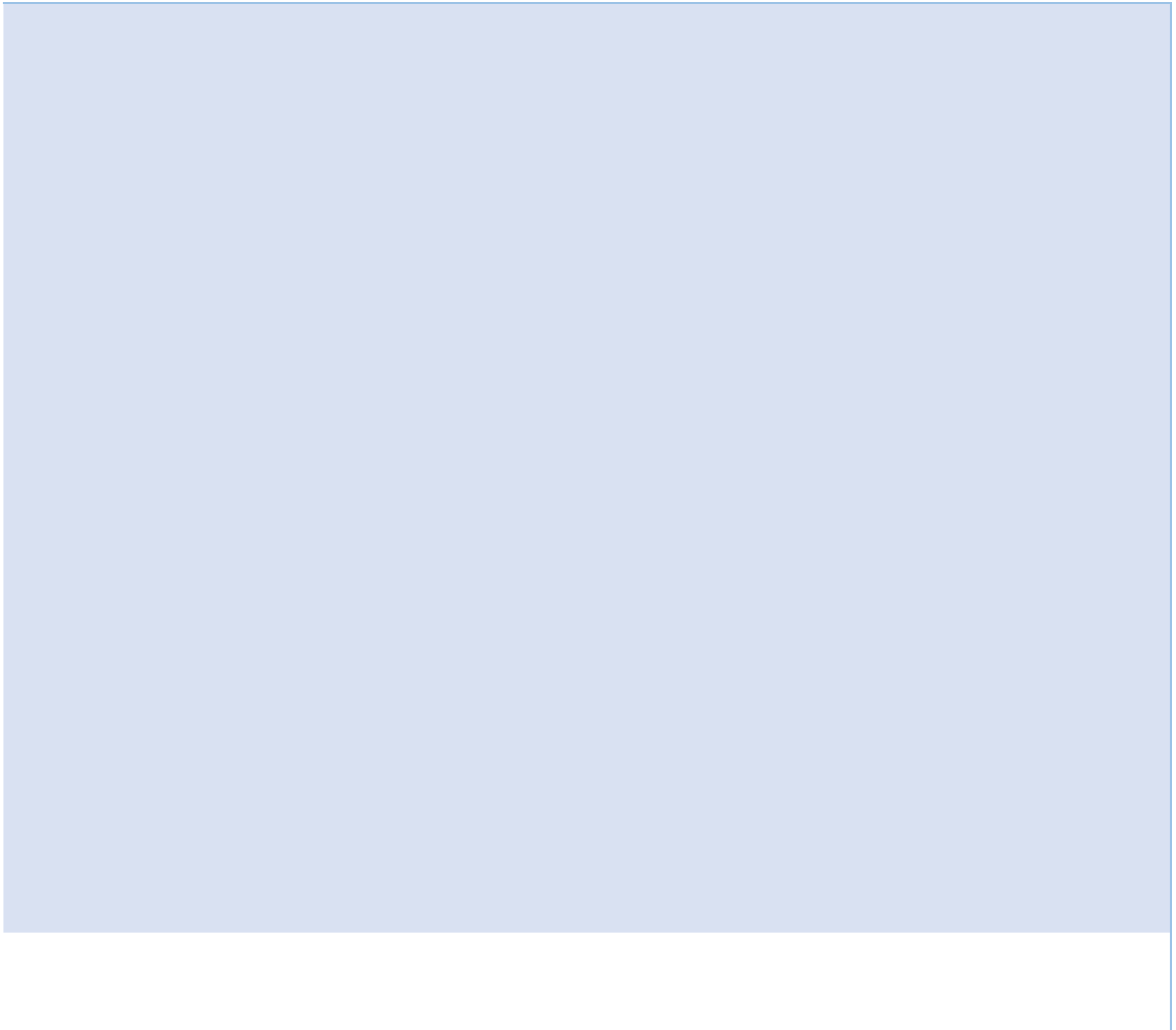


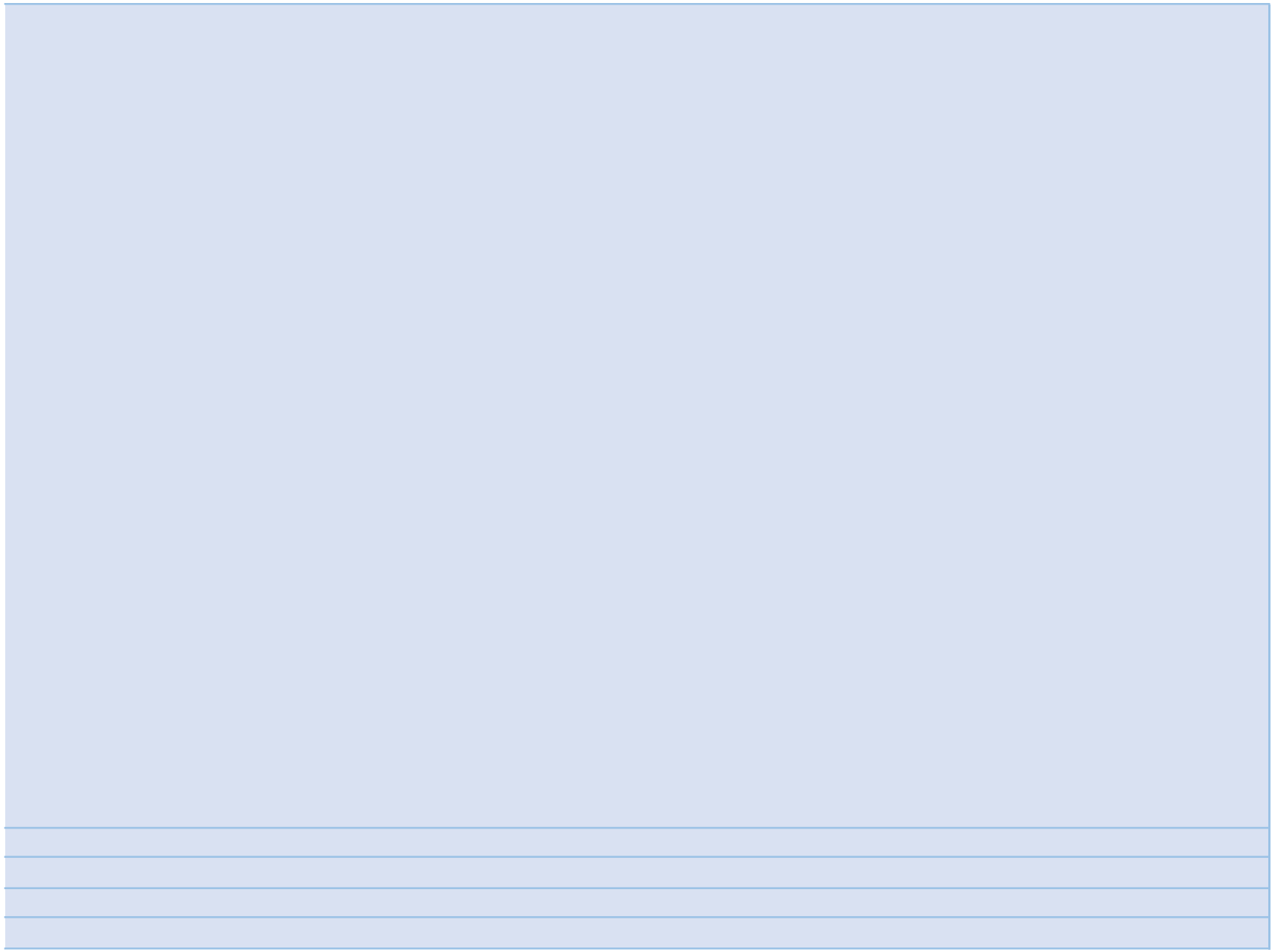


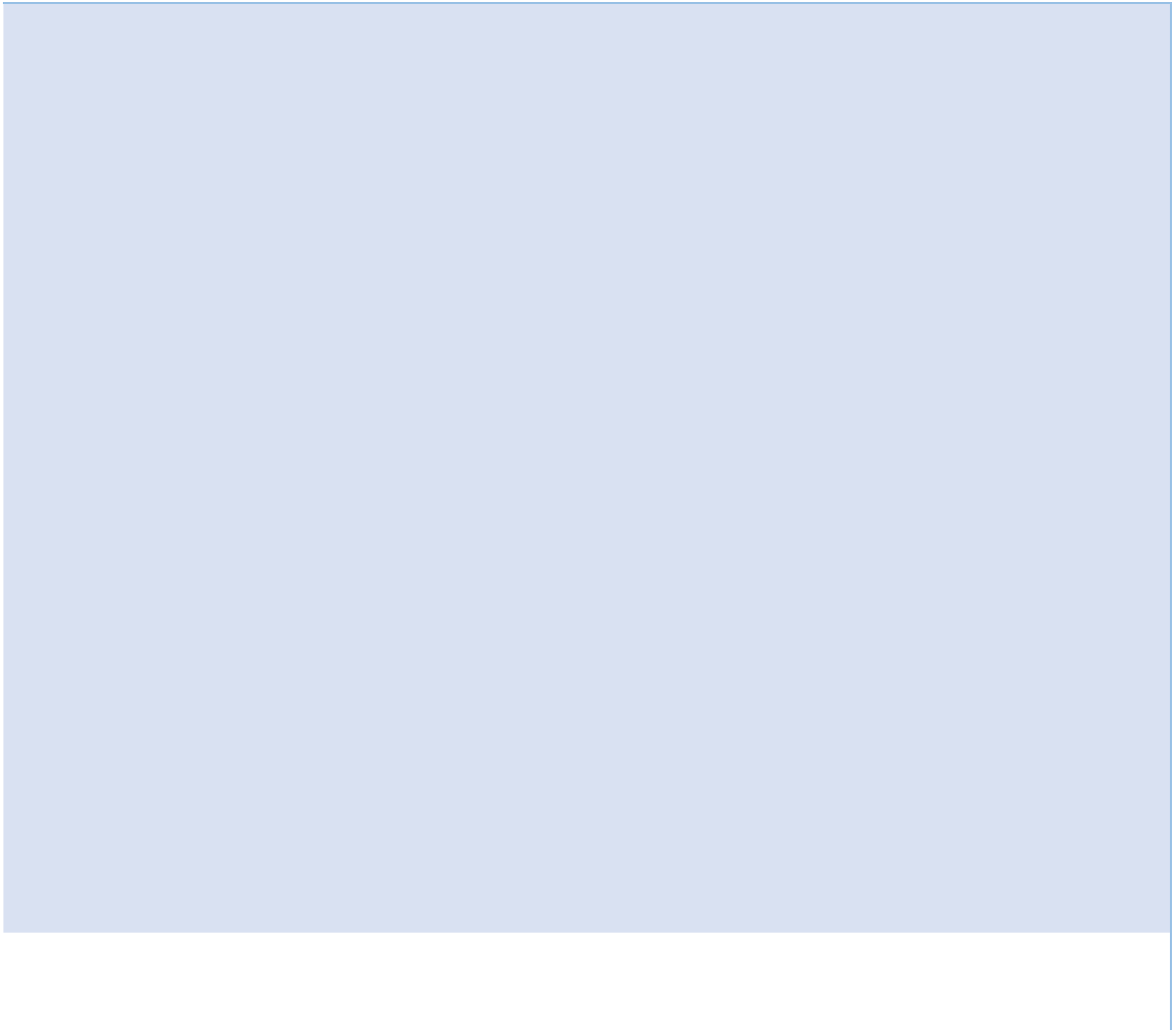












estic relationship,

ent brought an application for a protection order against the appellant pursuant to section 4(1) of the Act.

espondent and the appellant are in a "domestic relationship" as defined in the Act. Secondly, by erroneously finding that the appella

URN Number	Manage
4702024FCV001046	
4702024FCV001046	

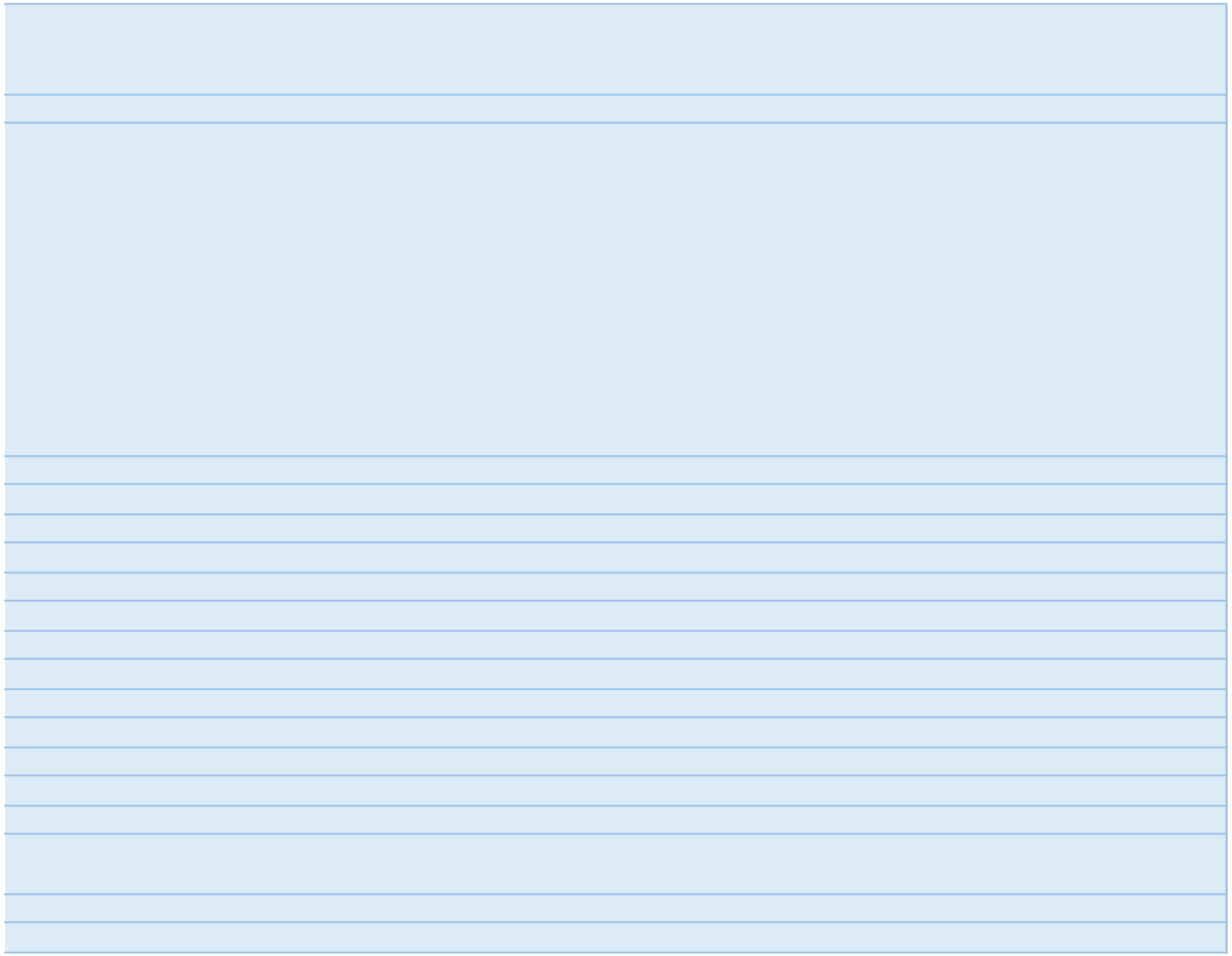
tshingombe tshitadi	8/6/2024	I m student ID applied appeal home affairs work permit conditions,school irregularity and back log	In Progress	1/15/2025

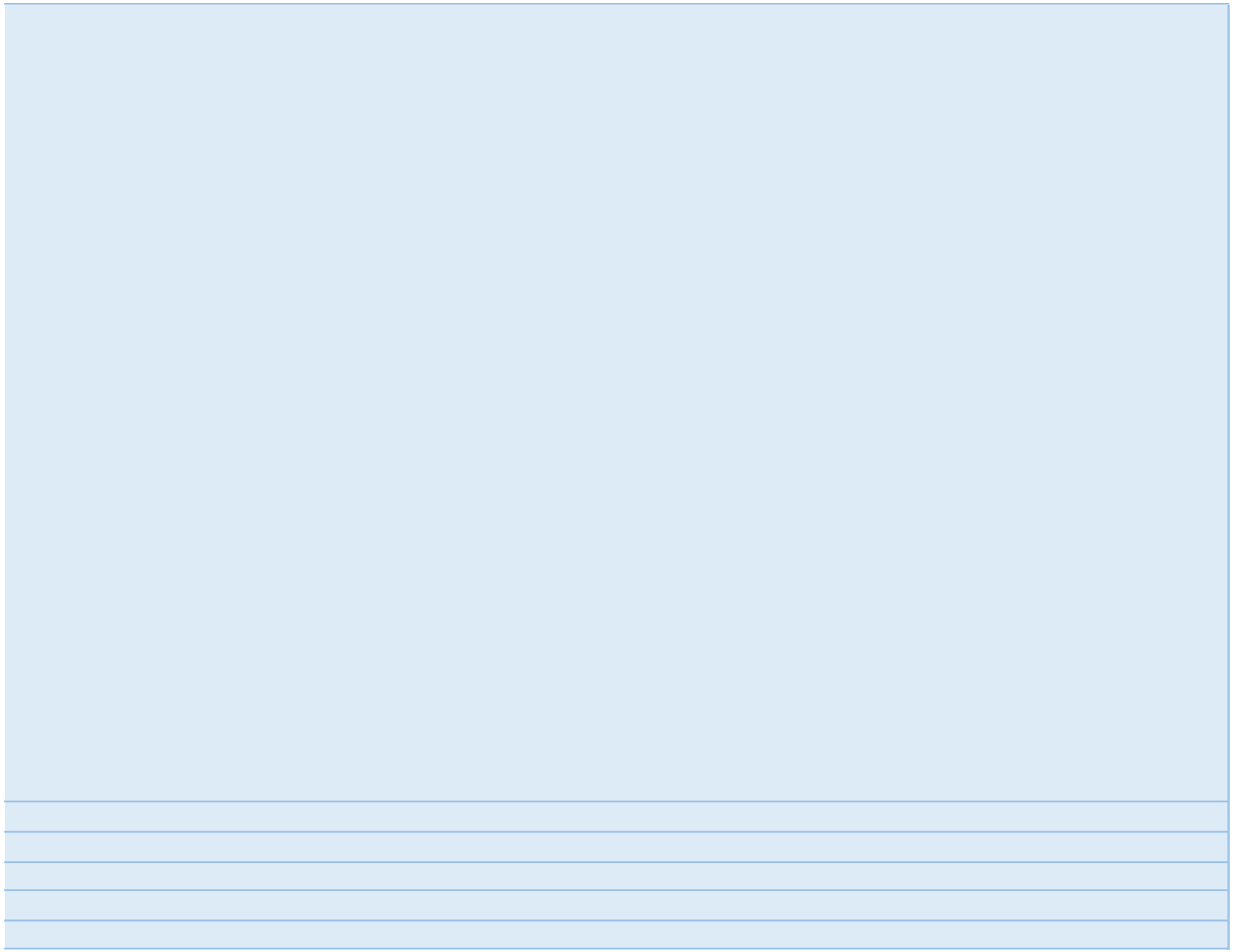
tshingombe tshitadi	7/22/2024	My query was conflic in civil procedure between system non resolution system agreement between national provide fund award ruling rescission Ccma and certified outcome transcript no agreement in work skill developmen t,my training college was irregularity and back log saga	In Progress	1/15/2025

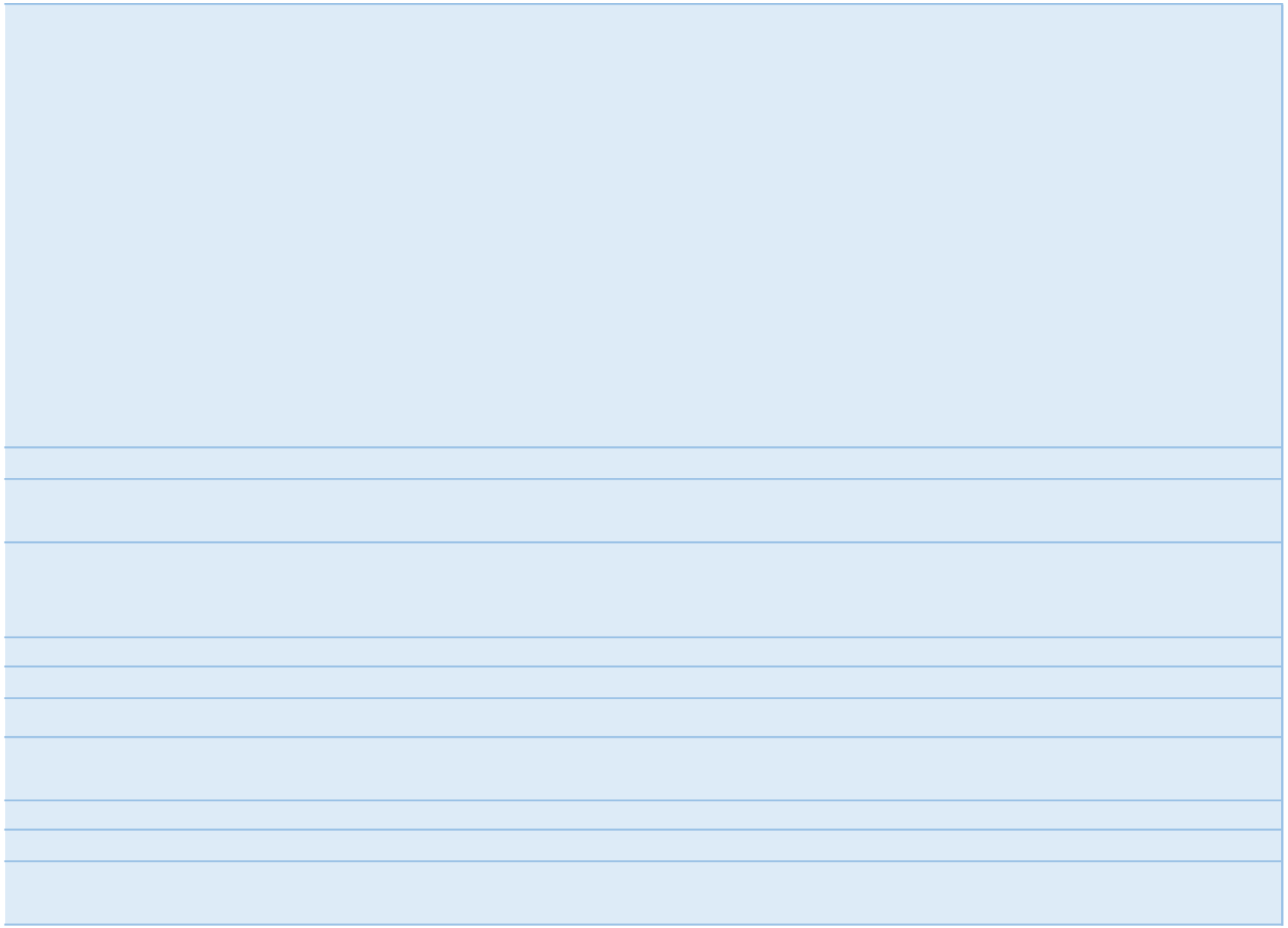
tshingombe tshitadi	7/22/2024	Hello dear court ,I' m ,notice motion referral / complain for my case number civil litigation ,Ccma granted review Gaek gbj 6806. labour case number jr 2461/15 record transcription certificate judgement appeal court order ,JA 17/19 notice petition labour court applicant Mr:	In Progress	1/15/2025

tshingombe tshitadi	7/22/2024	Hrllo criminal case complain on hilbro police station docket police close case number	In Progress	1/15/2025
URN	**Manage**			
1042024 CIV004539				
1042024 CIV004511				

112024CI V000013
112024CI V000012
112024CI V000011
112024CI V000014
112024CI V000015
112024CI V000009
112024CI V000008
112024CI V000006
112024CI V000007
112024CI V000005







of persons
ties

ryone can access it quickly on all devices. It is so much better than a POPI Act pdf. You can also link to (or share) a specific section. W
ework or join a Data Protection Programme and working through the POPIA lens to help you take the necessary action to comply.

vember 2013. The commencement date ofsection 1, Part A of Chapter 5, section 112 and section 113 was 11 April 2014. The comm

uropean Union aimed at protecting individuals' right to privacy. More specifically, the Act aims to give effect to the right to privacy
, e.g., someone's physical address, email address, date of birth, ID number, race, gender but also their criminal, financial and emplo
ning children; religious or philosophical beliefs; race or ethnic origin; trade union membership; political persuasion; health, sex life o
ereof.

esponsible party') might have about job applicants, employees and former employees (referred to as 'data subjects'). The Act impos

oyee.
of the information are.
an employment contract).
. This means, e.g., that personal information collected from an unsuccessful applicant should be destroyed after the recruitment pr

ete.
authorised access.

rrected if it is found to be inaccurate.

pay an employees' wage or salary; or for vetting relevant educational qualifications;

und to which the employee belongs or is required to belong; and

inal record of someone who requires security clearance; or providing information to an external party whom the employee has aut

se control); or

e Employment Equity Act which permits medical testing only if it is required or permitted by legislation or if it can be justified in the

ssed or acquired by an unauthorised person, i.e., someone who does not have consent to process the information. They also have t

pending on the nature and seriousness of a transgression.

rson needs to become familiar with the broad purposes of the Act and their responsibilities in terms of it.

for;

ategories of recipients personal information may be supplied;

emented and monitored to ensure that the information is not accessible by unauthorised people.

nt to disclosure of information as authorised in terms of the Act.

d for how long it has been held.

nformation Officer should be able to register with the Information Regulator any time from 1 May 2021.

. There are several steps that need to be taken, but these should be relatively easy to implement. The approach that an employer ta
outh Africa, a country where the right to be safe and free is enshrined in our Constitution. The judicial system encompasses 2 types o
n the alleged abuser by either the sheriff of the Court or a Police official.

he Respondent), to stop the abuse. This includes a roommate who shared a common residence. It's a legal document issued by a M

ighbour (the Respondent) and who doesn't share a common residence, to stop the harassment or abuse. It's a legal document issu

ence or the victims place of employment or where the victim resides; committing any other act as specified in the protection order i

commit any such act.

possible supported by an Affidavit setting out in detail what the Respondent did and on what date this incidents happened.

rm 2 as accurate as possible supported by an Affidavit setting out in detail what the Respondent did and on what date this incidents happened

so it supports the application for a protection order.

type of domestic abuse that's also a crime, then you can apply for a protection order, lay a criminal charge, or both. Some example

the application. The court in its discretion will issue an interim protection order after a court date has been issued to the Responde

at which the final order will be considered. Only once the final order is made, it will be permanent and can only be changed by app

f the Application is opposed. If the Respondent decides not to oppose the Application, no further action is needed.

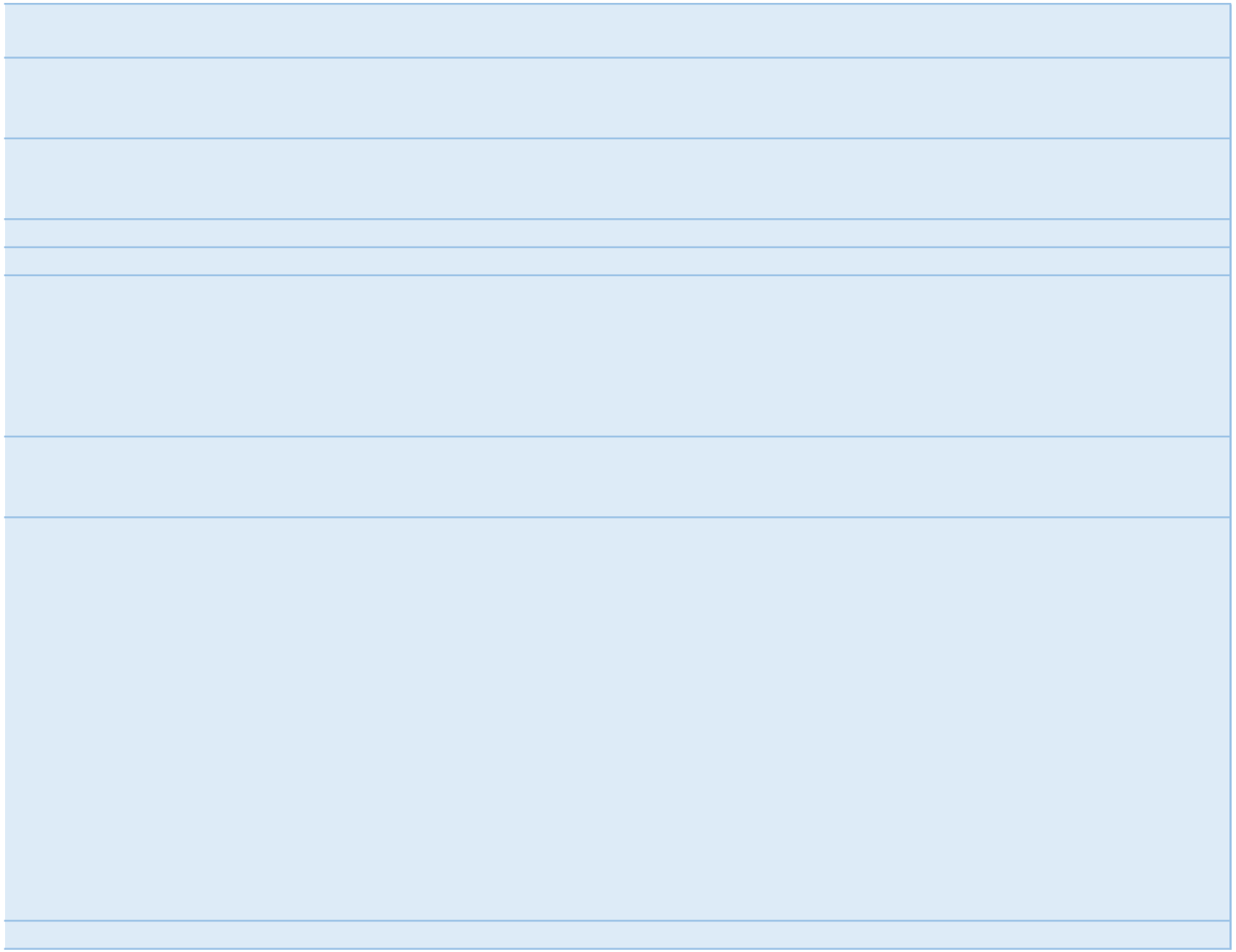
breaks the conditions of the protection order, the complainant/victim is obliged to go to the police station and open a criminal cas

ntenced to prison for not more than 5 years.

ook place and thus documenting the abuse thoroughly as this will give the presiding officer the necessary evidence to grant an Inte

e. Police officials are employed in terms of the South African Police Service Act, 1995 (Act No 68 of 1995). Civilian employees are

NO



A. PERSONAL PARTICULARS

	Tshingombe tshitadi
	Tshingombe
	Tirc000910610

	Officer engineering /assessment

22024-11-09

	WORK ADDRESS
	Haris markadet street st peace college

725298946
725298946

	WHITE	M	F	COLORED
	MARRIED			

	NO>>	CODE
	YES	

NO

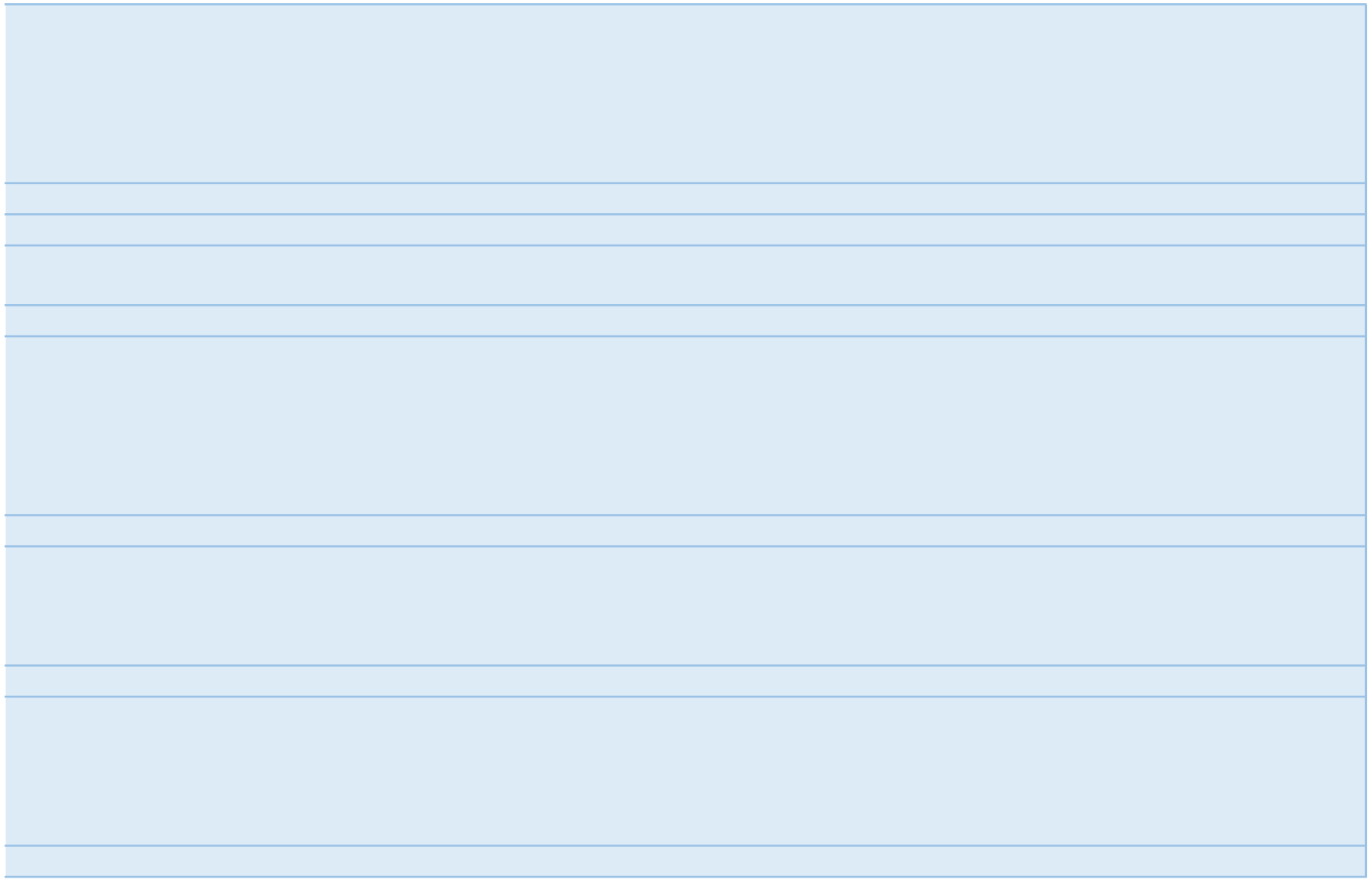
YES	NO>>>
ACKAGE	VOLUNTARY RESIGNATION

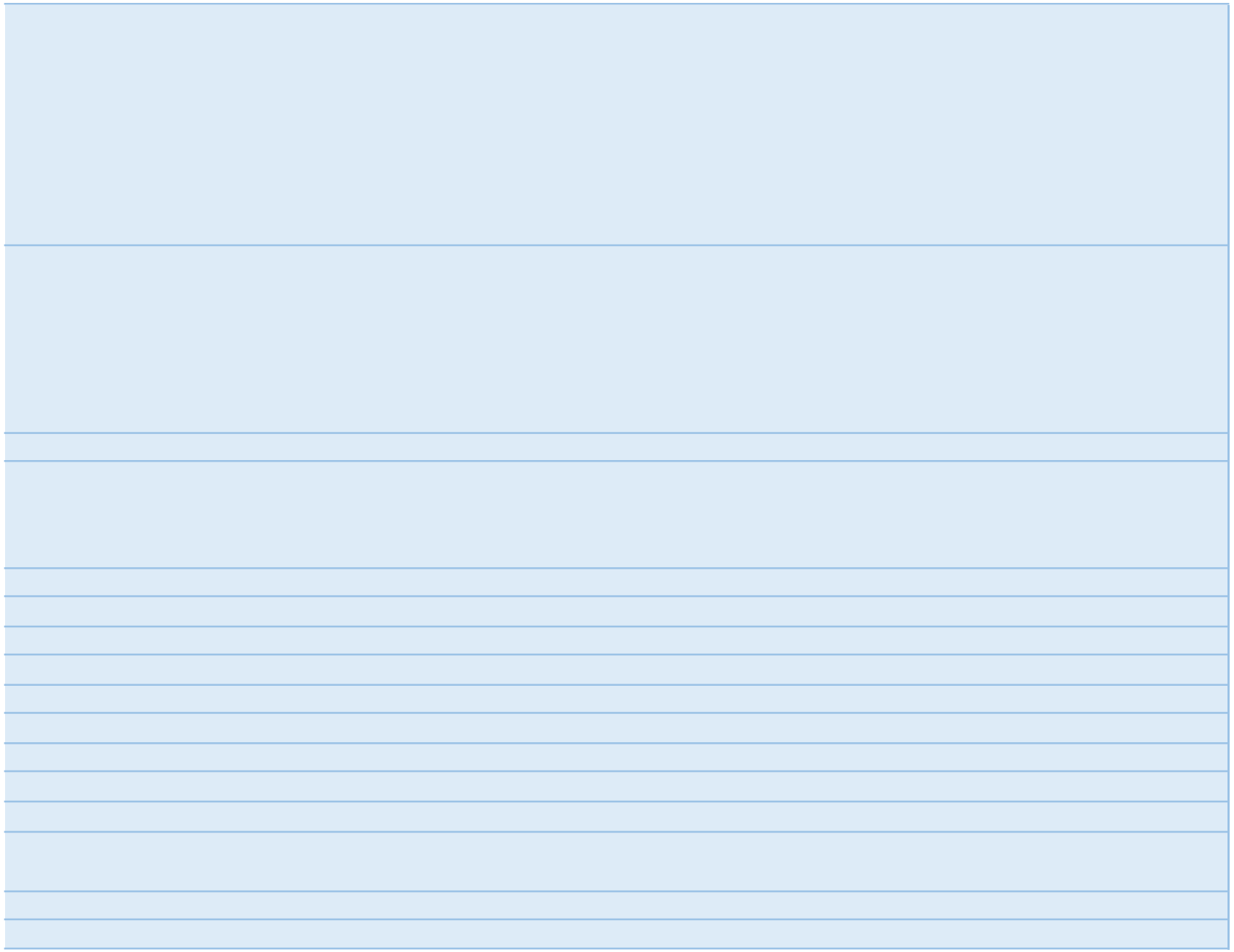
2/4/2025		
Ccma labour nogada		
	YES	NO>>
YES>>		N
KECUTION OF ANY OFFICIAL DUTIES, SHOULD	YES>>	NO
YES>>>		NO
YES>>>		NO
YES		NO>>
ADMISSION OF GUILT		
AMOUNT: R.....		
YES>>>>		NO
R PROTECTION FROM HARASSMENT ACT, 2011 (ACT NO 17 OF	YES>>>	NO

G. PARTICULARS OF WORK REFERENCES (NOT RELATIVES)

	NAME:section one
	ADDRESS OF COMPANY:
	Den vale
	EMAIL:info@section protection .co.za

						POSTAL CODE		
						TEL. HOME		
						TEL. WORK		
						CELL.		

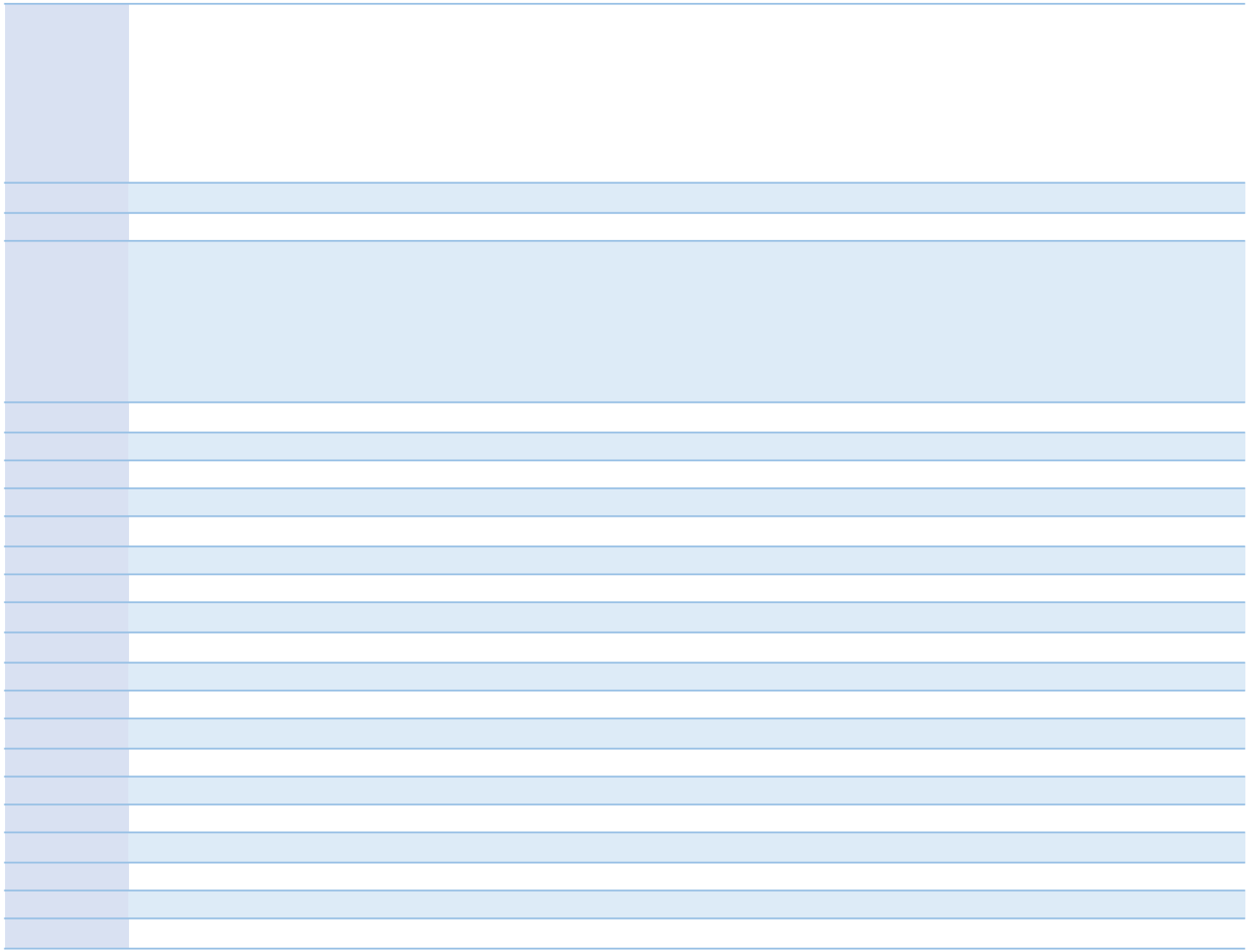


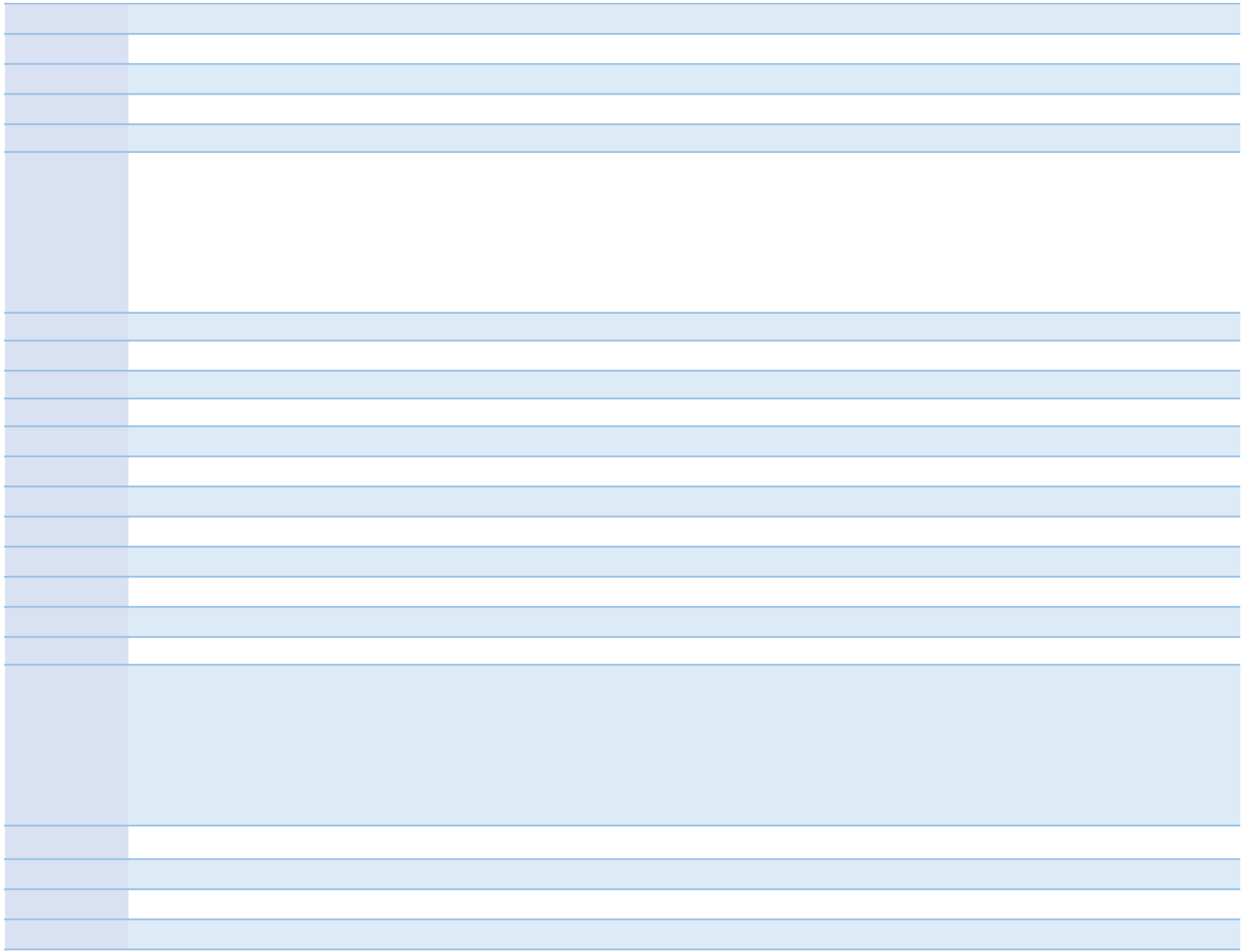


.....tshin gombe tshitadi ....

Column18	Column19	Column20	Column21	Column22	Column23	Column24	Column25	Column26	Column27

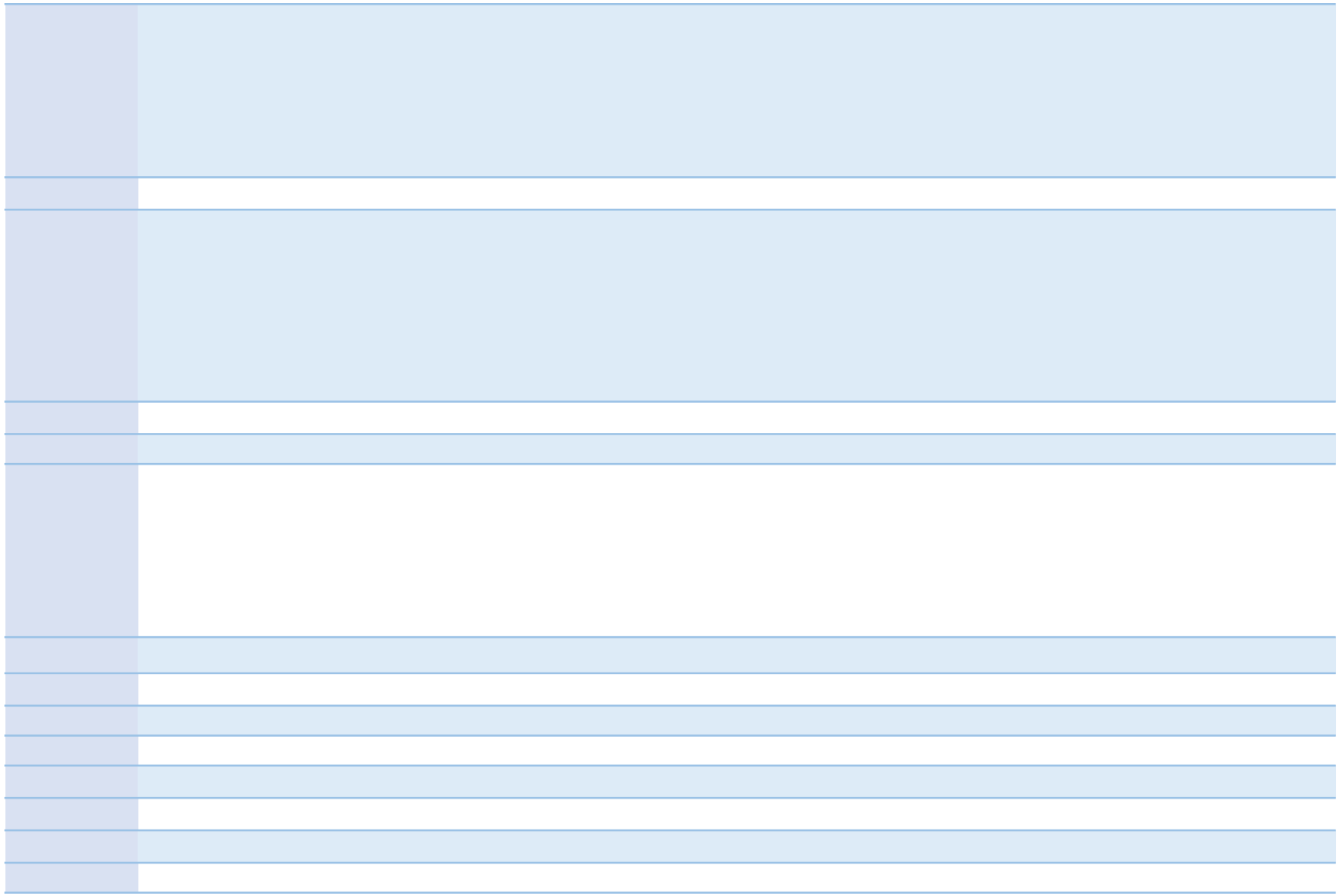
eir experimental implications.





al performance, **traffic management**, **investigation principles**, and **firearm study materials**. Here's a detailed breakdown of these t

pics:



ıd key topics:

ɔll, Kevin Stine. (Sep, 2011)

ɔll, Kevin Stine. (Sep, 2011)

urity concepts as you build confidence for exam day.

our pledge to help close the cybersecurity workforce gap and diversify those working in the field. To meet every learner’s needs, we’ı

th the confidence that you have a solid grasp of the right technical concepts, and a demonstrated aptitude to learn on the job. As an I

et of Things (IoT))

ıc.

; techniques to maximize your time and content retention.
/ards your ISC2; certifications. (Note: Credits may be eligible for continuing education credits for non-ISC2 certifications. Please review

administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrit

›gram.

P experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/SSCP/SSCP-Experience-Requi

ıgaged in the profession defined by the SSCP. The results of the JTA are used to update the examination. This process ensures that car

ıc.

n about acceptable IDs please visit: https://www.isc2.org/Exams/Exam-Day and look under What You Need to Bring to the Test Center tab for m

rification on the day of your test and on your future test days, detecting and preventing any fraud, and maintaining the security and integrity of t

Cybersecurity initiative, you willnot be able to register again with that code

urity initiative, you willnot be able to register again with that code.

ot be permitted to sit for any ISC2 examination.

tion at a later date you will be required to re-register for the exam and pay all applicable registration fees.

prior to releasing exam results. For the small number of candidates affected by this process, it is expected that candidates will receive
d, reviewed, or revisited.

ase visit https://www.isc2.org/Register-for-Exam and look under the Requesting Special Accommodations tab for information and instructions o

hinkEdge portfolio is enabling AI-driven applications in manufacturing sites, retail stores, schools, and more. Join @Flynn Maloy, Chief

a go-to language thanks to its easy-to-understand code and versatility. Today, Python can boast a wide array of libraries and framew

ientist to help…

ıl will leverage cutting-edge AI and robotics technologies...

will leverage...

In addition, please add msresearchforum@eventcore.com to your ‘safe sender’ list to ensure you receive future communications for t

er 285867147.

er 285867147.

nt's alleged denial of the respondent's version of events bears no evidential weight and falls to be rejected

Ve hope it empowers you and you find it helpful. This is POPIA (or the POPI Act) as enacted by the South African Parliament, but we hav

encement date of the other sections was 1 July 2020 (with the exception of section 110 and 114(4). The President of South Africa has

as provided for in the Constitution’s Bill of Rights by limiting the extent to which personal information may be processed by others, incl
yment history, personal opinions or beliefs, trade union membership, etc.
r biometric data of a data subject (finger printing, blood typing, voice recognition); and criminal behaviour in certain instances.

ses several new responsibilities on employers:

ocess has been finalised and a successful candidate appointed.

horised to carry out deductions from her or his wage or salary.

light of medical facts, employment conditions, social policy, or the fair distribution of employee benefits or the inherent requirement

the right to establish what information an employer holds and to request access to such information; to request the correction, destru

akes, may vary depending on the nature and size of the
of Protection Orders 1. the Domestic Violence Act 116 of 1998 (hereinafter referred to as the 'DPO') and 2. the Protection from Harassm

lagistrate in the jurisdiction area in which the abuse occurred that specifies the conditions that an abuser must adhere to, as specified

ed by a Magistrate in the jurisdiction area in which the abuse occurred that specifies the conditions that an abuser must adhere to, as

ncluding an order to seize any firearms or dangerous weapon from the Respondent; or

d.

es of abuse that are also crimes include common assault, rape, incest, attempted murder, and the abuse of animals

ent.

lying to the courts.

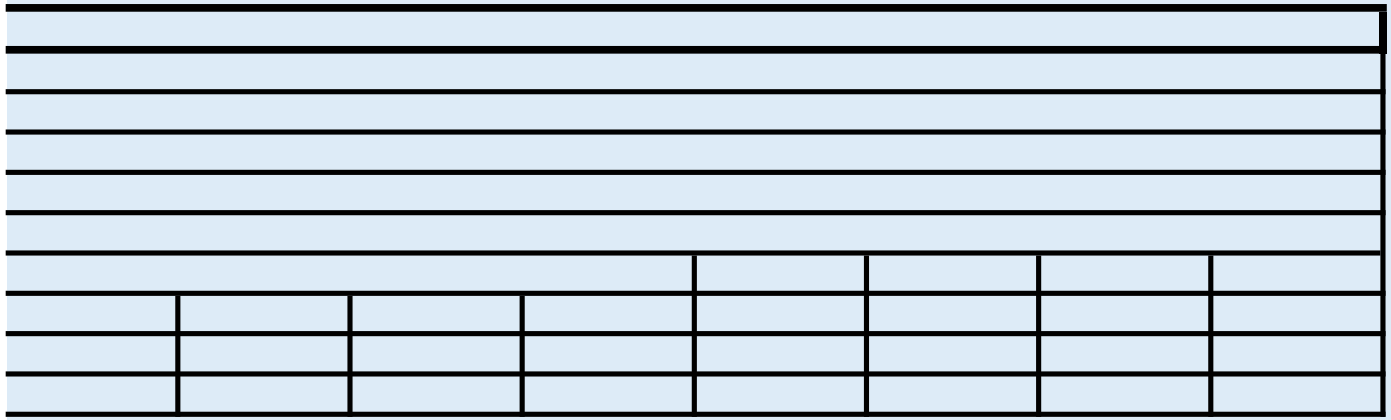
e. The complainant must file an affidavit and in an explicit manner and include all forms and dates of abuse in the affidavit. The Respo

rim Order against the Abuser. One should further avoid using a Protection Order maliciously, unreasonably and or vexatiously to obtai

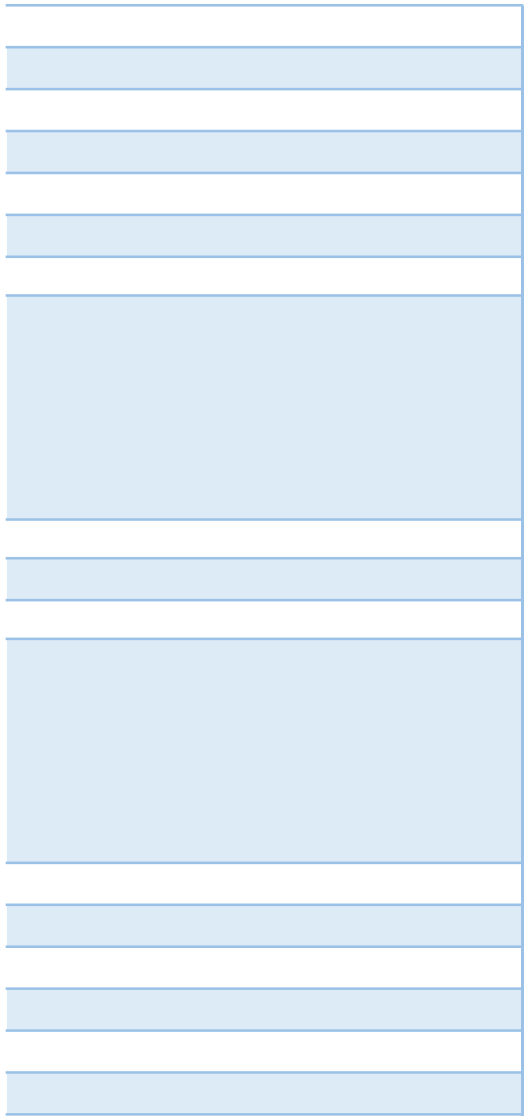
employed in terms of the Public Service Act, 1994 (Act No 103 of 1994). Most functional Police Officials are directly involved in pre

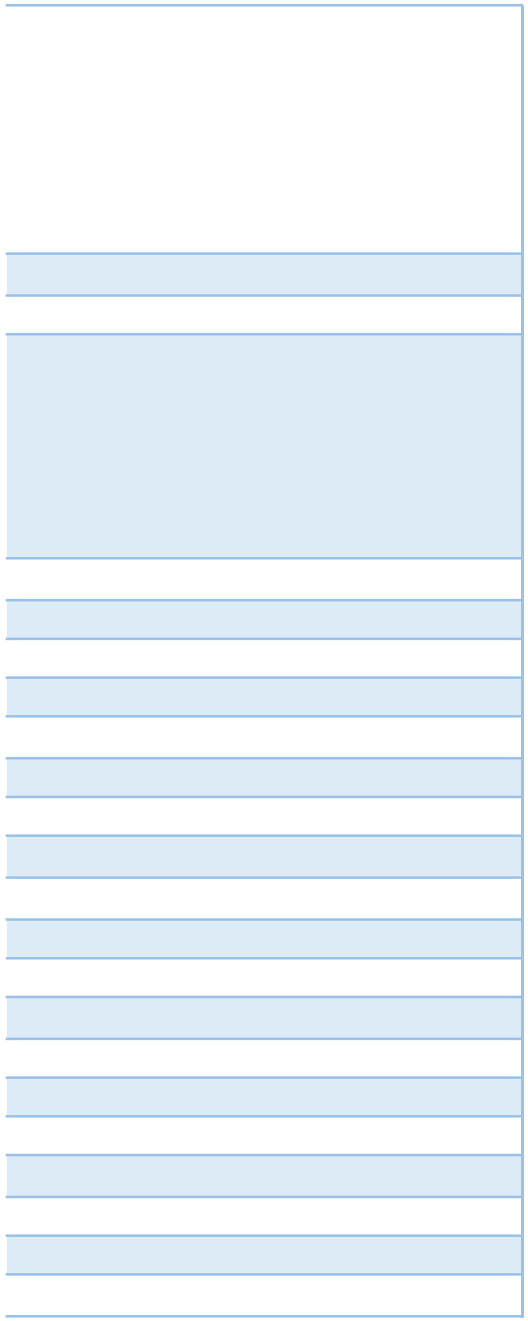
AGE	42
TITLE	Engineering electrical portofolio student
YES ..>	NO

	M	F
SINGLE>>		
		NO>>>
PSYCHOLOGICALLY		YES
YES		



Column28	Column29	Column30





opics and their experimental applications:

re also offering two CC Training Bundles with special extras. L

SC2 certification, those who hold the CC are backed by the w

/ the requirements established by the credentialing organizat

y and availability

rements

ıdidates are tested on the topic areas relevant to the roles ar

ıore information

the testing program. For more information on Pearson VUE‘s polic

e their results within 6 -8 weeks following the exam

n how to request an accommodation. Test accommodations are ir

f Marketing Officer of Lenovo ISG, as he details how Lenovo a

vorks, and they are the cornerstone of fast and easy Python

this event.

e reformatted it in the form of a website. The English text wa

proclaimed the POPI commencement date to be 1 July 2020.

uding employers.

s of the job. Testing for an employee's HIV status is prohibite

uction or deletion of personal information; to object on reaso

nent Act 17 of 2011 (hereinafter referred to as the ‘HPO’). It i

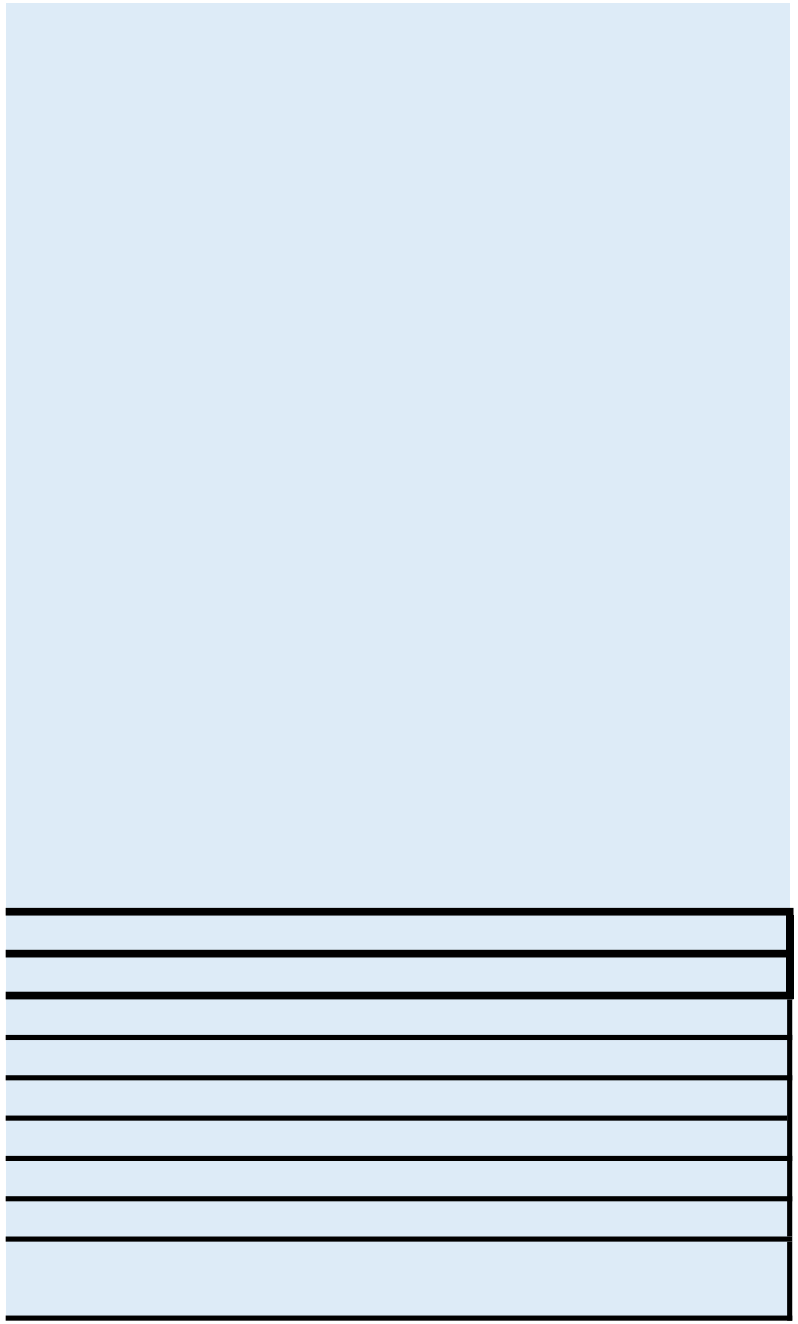
by the courts

specified by the courts

ndent will then be criminally charged with contempt of court

in an upper hand in a litigation matter. If proven that one act

venting, combating or investigating crime. The other Police o



	INDIAN	M	F
	DIVORCED		
VALID UNTIL			
		NO	
	NO>>>		